

Par les gosses battus, par l'ivrogne qui rentre
 Par l'âne qui reçoit des coups de pied au ventre
 Et par l'humiliation de l'innocent châtié
 Par la vierge vendue qu'on a déshabillée
 Par le fils dont la mère a été insultée

Je vous salue, Marie¹

To Theres and Seraina, to the memory of Marta

ON CM \mathbb{Z}_p -EXTENSIONS AND THE LEOPOLDT CONJECTURE FOR CM FIELDS

PREDA MIHĂILESCU

ABSTRACT. We show that Leopoldt's conjecture holds in CM fields. For the proof we construct a $CM\mathbb{Z}_p$ -extension of some CM field in which the Leopoldt conjecture is supposed to fail, and using the classes of primes which are completely split in this extension, we derive a contradiction. The method of proof can be described as a *stability check of Λ -modules under deformations in Thaine shifts*.

CONTENTS

1. Introduction	2
1.1. Notation and questions	2
1.2. Plan of the proof	5
2. Growth, stability and decomposition of Λ -modules	6
2.1. Kummer extensions, Property F and stabilization	10
2.2. Decomposition	13
2.3. On CM \mathbb{Z}_p -extensions of number fields	17
3. The main Theorem	19
3.1. Thaine shift and the main coherent sequences	21
3.2. Cohomology and the Hasse obstruction module	24
3.3. Completion of the auxiliary constructions	27
3.4. Proof of the main Theorem	31
4. Appendix : Proof of Proposition 3	32
References	33

¹Francis Jammes: *Prière*. Music by Georges Brassens

Date: Version 1.0 March 31, 2014.

Key words and phrases. 11R23 Iwasawa Theory, 11R27 Units.

1. INTRODUCTION

Let p be an odd rational prime and \mathbb{K}/\mathbb{Q} be a finite galois CM extension with group Δ , of which we shall assume that it contains the p -th roots of unity. We denote by \mathbb{K}_∞ the cyclotomic \mathbb{Z}_p -extension of \mathbb{K} and \mathbb{L} any other \mathbb{Z}_p extensions. The intermediate fields will be \mathbb{K}_n , resp. \mathbb{L}_n .

If \mathbb{L}/\mathbb{K} is an arbitrary \mathbb{Z}_p -extension, with group $\Gamma \cong \mathbb{Z}_p$, generated by $\tau \in \Gamma$ as a topological generator, the Iwasawa algebra is $\Lambda = \mathbb{Z}_p[[T]]$, $T = \tau - 1$. The intermediate fields are $\mathbb{L}_n \subset \mathbb{L}$ and, if $\mathbb{L} = \mathbb{K}_\infty$ is the cyclotomic \mathbb{Z}_p -extension, then we always assume that $\mathbb{K}_n = \mathbb{L}_n$ contains exactly the p^n -th roots of unity, but not the p^{n+1} -th ones; this can be achieved by an adequate numeration, at least for some sufficiently large n .

We write $\tau_n = (T + 1)^{p^{n-k}}$ for the power of τ that generates the fixing group of \mathbb{K}_n , and $\omega_n = \tau_n - 1$; $\nu_{n+j,n} = \omega_{n+j}/\omega_n$, $j > 0$. The p -parts of the ideal class groups of $\mathbb{K}_n, \mathbb{L}_n$ are $A_n = A(\mathbb{K}_n), A(\mathbb{L}_n)$ and $A = A(\mathbb{K}) = \varprojlim_n A(\mathbb{K}_n), A(\mathbb{L}) = \varprojlim_n A(\mathbb{L}_n)$; the groups A'_n, A' are defined like A_n, A , with respect to the ideal classes of the p -integers of $\mathbb{K}_n, \mathbb{L}_n$. The groups $B_n \subset A_n$ are the maximal subgroups generated by classes containing ramified primes above p and $B = \varprojlim_n B_n$, while $A' = A/B$. We note that the base field \mathbb{K} can be modified within the same \mathbb{Z}_p -extension, by replacing \mathbb{K} with \mathbb{K}_n , say. As a consequence, the Iwasawa algebra may become $\Lambda' = \mathbb{Z}_p[[\omega_n]]$.

1.1. Notation and questions. For arbitrary number fields \mathbb{K} , the cyclotomic \mathbb{Z}_p -extension is denoted by \mathbb{K}_∞ . In some parts of this paper we shall consider also a further \mathbb{Z}_p -extension \mathbb{L}/\mathbb{K} , setting some important additional conditions on the intersection $\mathbb{L} \cap \mathbb{K}_\infty$. In such context we encounter at least two different Iwasawa algebras; additional variation can result from changing the base field as mentioned above. We restrict our introductory notation and remarks to the above; the precise choices and adequate notations for combined extensions will be introduced in the given context. Here we still restrict to the context of one single, not necessarily cyclotomic, \mathbb{Z}_p -extension \mathbb{L}/\mathbb{K} and introduce some additional concepts and notations.

Definition 1. For $f \in \mathbb{Z}_p[T]$ a distinguished polynomial and M an additively written Λ -torsion module, we write

$$\begin{aligned} M(f) &= \{a \in A : \exists m : f^m(T)a = 0\} \quad \text{and} \\ (1) \quad M[f] &= \{a \in A : f(T)a = 0\}. \end{aligned}$$

If X is a finite abelian p -group, its exponent is $\exp(X) = \min\{p^m : p^m X = 0\}$. The subexponent is the smallest size of a cyclic direct summand in X , thus $\text{sexp}(X) = \min\{\text{ord}(x) : x \in X \setminus pX\}$.

We let $F(A) \subset A$ be the maximal finite Λ -submodule of A , while A° denotes the \mathbb{Z}_p -torsion submodule, so $F(A) \subset A^\circ$.

If \mathbb{K} is a number field, we denote its units by $E(\mathbb{K}) = \mathcal{O}^\times(\mathbb{K})$. Dirichlet's unit theorem states that, up to torsion made up by the roots of unity

$W(\mathbb{K}) \subset \mathbb{K}^\times$, the units $E = \mathcal{O}(\mathbb{K})^\times$ are a free \mathbb{Z} - module of \mathbb{Z} - rank $r_1 + r_2 - 1$. As usual, r_1 and r_2 are the numbers of real, resp. pairs of complex conjugate embeddings $\mathbb{K} \hookrightarrow \mathbb{C}$. We consider the set $P = \{\wp \subset \mathcal{O}(\mathbb{K}) : (p) \subset \wp\}$ of distinct prime ideals above p and let

$$\mathfrak{K}_p = \mathfrak{K}_p(\mathbb{K}) = \prod_{\wp \in P} \mathbb{K}_\wp = \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p$$

be the product of all completions of \mathbb{K} at primes above p . Let $\iota : \mathbb{K} \hookrightarrow \mathfrak{K}_p$ be the diagonal embedding. We write $\iota_\wp(x)$ for the projection of $\iota(x)$ in the completion at $\wp \in P$. If $y \in \mathfrak{K}_p$, then $\iota_\wp(y)$ is simply the component of y in \mathbb{K}_\wp . If $U \subset \mathfrak{K}_p^\times$ is the group of units, thus the product of local units at the same completions, then E embeds diagonally via $\iota : E \hookrightarrow U$.

Let $\overline{E} = \overline{\iota(E)} = \bigcap_{n \geq 0} \iota(E) \cdot U^{p^n} \subset U$ be the p -adic closure of $\iota(E)$; this is a \mathbb{Z}_p - module with $\mathbb{Z}_p\text{-rk}(\overline{E}) \leq \mathbb{Z}\text{-rk}(E) = r_1 + r_2 - 1$. The difference

$$\mathcal{D}(\mathbb{K}) = \mathbb{Z}\text{-rk}(E) - \mathbb{Z}_p\text{-rk}(\overline{E})$$

is called the *Leopoldt defect*. The defect is positive if, in the idelic embedding, units which are \mathbb{Z} -independent, are related p -adically. Equivalently, if the p - adic regulator of \mathbb{K} vanishes.

Leopoldt suggested in [12] that $\mathcal{D}(\mathbb{K}) = 0$ for all number fields \mathbb{K} . This conjecture of Leopoldt was proved for abelian extensions by Brumer [4] in 1967, using a result of Ax [1] and a local version of Baker's linear forms in logarithms [3]. It is still open for arbitrary non abelian extensions. Since 1967 various attempts have been undertaken for extending the results of [4] to non abelian extensions, using class field theory, Diophantine approximation or both. The following very succinct list is intended to give an overview of various approaches, rather than being an extensive list of results on Leopoldt's conjecture. In [7], Greenberg notes a relation between the Leopoldt Conjecture and a special case of the Greenberg Conjecture: he shows that Leopoldt's Conjecture implies that $A(T)$ (see §1.1. for the definitions) is finite for totally real fields, i.e. the Greenberg Conjecture holds for the T - part.

Emsalem, Kisilevsky and Wales [5] use group representations and Baker theory for proving the Conjecture for some small non abelian groups; this direction of research has been continued in some further papers by Emsalem or Emsalem and coauthors. Jaulent proves in [10] the Conjecture for some fields of small discriminants, using the *phantom* field Φ which we define in the Appendix. Currently the strongest result based on Diophantine approximation was achieved by Waldschmidt [16], who proved that if r is the \mathbb{Z} - rank of the units in the field \mathbb{K} , then the Leopoldt defect satisfies $\mathcal{D}(\mathbb{K}) \leq r/2$.

The connection of Leopoldt's conjecture to class field theory was already noted by Iwasawa in [8]. He shows that if $\Omega(\mathbb{K}) \supset \mathbb{K}_\infty$ is the maximal p -abelian p -ramified extension of \mathbb{K} , then $\text{Gal}(\Omega(\mathbb{K})/\mathbb{K}) \sim \mathbb{Z}_p^n$, where $n = r_2 + 1 + \mathcal{D}(\mathbb{K})$; the proof of this fact is in any text book on cyclotomy and

Iwasawa theory. For CM extensions \mathbb{K} , the contraposition of the conjecture herewith reduces to the statement that \mathbb{K}^+ has more \mathbb{Z}_p -extensions than just the cyclotomic one. It is this assumption which we shall use and lead to a contradiction. If Leopoldt fails thus for \mathbb{K}^+ and if $\mathbb{L}^+/\mathbb{K}^+$ is a further \mathbb{Z}_p -extension, it will be totally real and $\mathbb{L} = \mathbb{L}^+ \cdot \mathbb{K}$ will be a CM extension. Starting from this fact, we prove in this paper:

Theorem 1. *For odd primes p , the Leopoldt defect vanishes in arbitrary CM extensions \mathbb{K} .*

We shall use the following notations, for arbitrary fields \mathbf{K} : the maximal unramified p -abelian extension is $\mathbb{H}(\mathbf{K})$. If \mathbf{K} is CM, then complex conjugation acts on galois groups, and maximal extensions split naturally in plus and minus parts: for instance, $\mathbb{H}^+(\mathbf{K})$ is the subfield fixed by $\text{Gal}(\mathbb{H}/\mathbf{K})^{1-j}$, with $j \in \text{Gal}(\mathbf{K}/\mathbb{Q})$ the restriction of complex conjugation to this field. The maximal p -abelian, p -ramified extension is denoted by $\Omega(\mathbf{K})$ and $\mathbb{M}(\mathbf{K}) \subset \Omega(\mathbf{K})$ is the product of all \mathbb{Z}_p -extensions of \mathbf{K} , while $\mathbf{K}_\infty/\mathbf{K}$ is the cyclotomic \mathbb{Z}_p -extension.

For CM extensions we define $\mathbb{M}^+(\mathbf{K}) = \mathbb{M}(\mathbf{K}^+) \cdot \mathbf{K}$. The Leopoldt conjecture holds for \mathbf{K} iff $\mathbb{M}^+(\mathbf{K}) = \mathbf{K}_\infty$, and in general we have the rank equality

$$\mathbb{Z}_p\text{-rk}(\text{Gal}(\mathbb{M}^+(\mathbf{K})/\mathbf{K})) = \mathcal{D}(\mathbf{K}) + 1.$$

The term 1 on the right hand side stands for the cyclotomic \mathbb{Z}_p -extension, which is the only one which is expected to exist, if Leopoldt's conjecture is true. We note that $\mathbb{M}^+(\mathbf{K})$ is also the product of all CM \mathbb{Z}_p -extensions of \mathbf{K} and Leopoldt's conjecture thus claims that \mathbf{K} has only one CM \mathbb{Z}_p -extension, namely the cyclotomic one. The CM property of \mathbb{Z}_p -extensions plays a crucial role in our proof.

Remark 1. A. *If \mathbb{K}_{-1} is a field for which $\mathcal{D}(\mathbb{K}_{-1}) > 0$, then it is known that the same holds for arbitrary finite algebraic extensions $\mathbb{K}/\mathbb{K}_{-1}$; this is noted, for instance, by Laurent in the introduction to [11]. We shall use negative indices for designing number fields which will first be enlarged for certain purposes, before considering actual \mathbb{Z}_p -extensions. We thus keep the notation \mathbb{K} for base fields of the \mathbb{Z}_p -extensions of interest.*

It follows from the fact that the linear relations between \mathbb{Z} -generators of the units of $E(\mathbb{K}_1)$, which arise upon p -adic completion, will be preserved under the embedding into the units $E(\mathbb{K})$.

B. *If \mathbb{K} is a CM extension containing the p^m -th roots of unity and $\mathbb{L}^+/\mathbb{K}^+$ is a p -ramified cyclic extension of degree p^m , then there is a class $a \in A^-(\mathbb{K})$ such that $\mathbb{L}^+ \cdot \mathbb{K} = \mathbb{K}[a^{1/p^m}]$ in the sense that for each $\mathfrak{A} \in a$ there is an $\alpha \in \mathfrak{A}^{(1-j)p^m}$ with $\mathbb{L} = \mathbb{K}[\alpha^{1/p^m}]$. We shall use this notation for explicit Kummer extensions throughout the paper.*

The following result has been proved independently by Babaicev [2] and Monsky [13]:

Theorem 2. *Let \mathbb{K} be a number field and let \mathbb{M} be the product of all of its \mathbb{Z}_p -extensions. Then there is an absolute bound $B = B(\mathbb{K}) > 0$ such that for all \mathbb{Z}_p -subextensions $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, we have $\mu(\mathbb{L}) \leq B(\mathbb{K})$, where $\mu(\mathbb{L})$ is Iwasawa's μ constant for \mathbb{L} .*

It will be used in our proof for bounding the μ -constant for CM \mathbb{Z}_p -extensions.

1.2. Plan of the proof. The proof is inspired by a construction of Iwasawa for showing that there exist Λ -extensions with $\mu > 0$. We assume that K is some CM extension for which the Leopoldt defect does not vanish, and create first an auxiliary extension $\mathbb{K} \supset K$ which also has positive Leopoldt defect, together with some additional properties. We then construct a CM \mathbb{Z}_p -extension \mathbb{L}/\mathbb{K} with $\mathbb{L} \cap \mathbb{K}_\infty = \mathbb{K}_N$ for some large N , and such that there is a prime $\mathfrak{q} \in a_N \in A^-(\mathbb{K}_N)$ which is totally split in \mathbb{L}/\mathbb{Q} . The class a_N is induced by ideal lifts from an abelian extension \mathbf{k} that we can control. We then define $\mathbb{F} \subset \mathbb{Q}[\zeta_q]$ the subfield of degree p , with q the rational prime above \mathfrak{q} and let $\mathbb{L}' = \mathbb{L} \cdot \mathbb{F}$, an extension in which the split primes above \mathfrak{q} will ramify. The explicit construction is described in the first section of Chapter 3. If $x \in A(\mathbb{L})$ for some \mathbb{Z}_p -extension \mathbb{L}/\mathbb{K} , we distinguish the case when Λx is infinite of finite p -rank (the λ -type) or infinite of bounded order (the μ -type). Modules which can be split into cyclic submodules of the two kinds are called decomposed¹. We let $\mathfrak{Q}_n \subset \mathbb{L}'_n$ be norm coherent ramified primes above the split primes $\mathfrak{q}_n \subset \mathbb{L}_n$, above \mathfrak{q} . Letting $b_n = [\mathfrak{Q}_n^{1-j}]$, we show that the sequence of classes $b = (b_n)_{n \in \mathbb{N}} \in A^-(\mathbb{L}')$ must necessarily be indecomposed – otherwise a contradiction is easily obtained.

Growth and decomposition of Λ -modules play an important role in our proof, and they are investigated at length in the second chapter. We show in particular that we may choose \mathbb{K} such that $TA^-(\mathbb{L})$ is a decomposed module, for all CM - \mathbb{Z}_p -extensions \mathbb{L}/\mathbb{K} . Thus, the sequence is *not far* from being decomposed, and in fact we have $Tb = b_\lambda + b_\mu$. The ramification conditions will in fact imply that $b_\lambda \in \iota(A^-(\mathbb{L}))$. This particular condition will lead to a contradiction with the choice of \mathbf{k} , a contradiction which shows that the extension \mathbb{L} cannot exist.

The CM property of our extensions has an important contribution to the simplicity of the proof, in that capitulation is reduced to a \mathbb{Z}_p -cyclic, well understood submodule. This simplifications are treated in §2.4. The structure of b and its decomposition is governed by consequences of the construction and the Hasse Norm Principle. These consequences are derived in §3.2.

¹See below for the formal complete definition.

2. GROWTH, STABILITY AND DECOMPOSITION OF Λ -MODULES

In this section \mathbb{L}/\mathbb{K} is an arbitrary \mathbb{Z}_p -extension of the base-field \mathbb{K} , which is assumed to be galois over \mathbb{Q} and contain the p -th roots of unity, for simplicity. In addition, the primes above p are assumed to be completely ramified in \mathbb{L}/\mathbb{K} . In this section we develop several properties concerning the growth and stabilization of Λ -modules along intermediate extensions of a \mathbb{Z}_p -extension, as well as some properties of the module of decomposed elements. These properties will be used in the next chapter in order to define a particular tower of extensions with respect to which we shall perform the proof of the main Theorem. In both chapters, base fields will be denoted by \mathbb{K} or some related notation, and we consider one or more \mathbb{Z}_p -extensions thereof. In particular, the precise properties of the base field \mathbb{K} for which we perform the final proof, will be only given in the third chapter.

The Iwasawa algebra is defined like in the introduction and we recall that A is a finitely generated Λ -torsion module. We associate elementary modules to A as follows:

Definition 2. *Let A be a finitely generated Λ -torsion module and $\mathcal{E}(A) = \mathcal{E}(A)_\lambda \oplus \mathcal{E}(A)_\mu$ be an elementary Λ -module, with $\mathcal{E}(A)_\mu = \bigoplus_{i=1}^m \Lambda/(p^{e_i})$ and $\mathcal{E}(A)_\lambda = \bigoplus_{j=1}^n \Lambda/(f_j^{e_j})$. If $\mathcal{E}(A) \sim A$ are pseudoisomorphic, we say that the elementary module $\mathcal{E}(A)$ is associated to A . The μ -part $\mathcal{E}(A)_\mu$ is uniquely determined by A , while the distinguished polynomials $f_j \in \mathbb{Z}_p[T]$ and their exponents e_j occurring in $\mathcal{E}(A)_\lambda$ can vary.²*

The following notions are connected to Λ -modules:

Definition 3. *Let \mathbb{L}/\mathbb{K} be a \mathbb{Z}_p -extension and Λ the associated Iwasawa algebra. Let N be some finitely generated Λ -torsion module. We say that $a \in N$ is of λ -type, if Λa is infinite of finite p -rank and of μ -type if Λa is infinite of finite order. Finally a is of finite type, if Λa is finite. Accordingly, N is of one of the three types, if it is generated by elements of one of the three types. Note that modules of λ or μ -type can contain finite submodules.*

The maximal finite Λ -module is $F(N)$ while $M(N) := N^\circ$ is its \mathbb{Z}_p -torsion submodule. Note that $M(N)$ is at the same time the module of all elements which are either of μ - or of finite type. We let $L(N) = \{x \in N : p\text{-rk}(\Lambda x) < \infty\}$, the module of all elements that are either of λ - or of finite type.

An element $x \in A(\mathbb{L})$ is decomposable, if there are $x_\lambda \in L(A), x_\mu \in M(A)$, such that $x = x_\lambda + x_\mu$. It is indecomposable otherwise. If x is decomposable and $x = x_\lambda + x_\mu = x'_\lambda + x'_\mu$ are two decompositions, then $x'_\lambda - x_\lambda = -(x'_\mu - x_\mu) \in F(A)$. The submodule

$$D := \{x = y + z : y \in L, z \in M\} \subset A$$

is the module of decomposable elements.

²They can be fixed by assuming they are irreducible. However, such a choice can result in an increase of either kernel or cokernel, which might be undesirable in certain cases.

If \mathbb{H}/\mathbb{L} is the maximal abelian unramified extension of \mathbb{L} , we denote the Artin map by $\varphi : A(\mathbb{L}) \rightarrow \text{Gal}(\mathbb{H}/\mathbb{L})$. It is not difficult to see that $[A : D] < \infty$. Indeed, if $\psi : \mathcal{E}(A) \rightarrow A$ is a pseudoisomorphism, then $\text{Ker}(\psi) = 0$ since the kernel is finite and $\mathcal{E}(A)$ has no finite submodule. Thus $D' := \psi(\mathcal{E}(A)) \subset A$ is a decomposed submodule, thus $D' \subset D$. Since ψ is a pseudoisomorphism, the cokernel is finite so $\text{Coker}(\psi) = A/D'$ is finite. A fortiori, $[A : D] \leq [A : D'] < \infty$, so A/D is finite.

If $x \in A \setminus D$, the L - and the D -orders of x are, respectively

$$(2) \quad \begin{aligned} \ell(x) &= \min\{j > 0 : p^j x \in L\}, \quad \text{and} \\ \delta(x) &= \min\{k > 0 : p^k x \in D\} \leq \ell(x). \end{aligned}$$

We may associate the modules to the extension, writing $L(\mathbb{L}), M(\mathbb{L}), F(\mathbb{L})$ and note that the canonical submodules $L(\mathbb{L}), M(\mathbb{L}) \subset A(\mathbb{L})$ verify

$$(3) \quad D(\mathbb{L}) = L(\mathbb{L}) + M(\mathbb{L}), \quad L(\mathbb{L}) \cap M(\mathbb{L}) = F(\mathbb{L})$$

Throughout the paper, unless otherwise specified, the distinguished polynomial $F(T) \in \mathbb{Z}_p[T]$ will denote the minimal annihilator polynomial of $L(\mathbb{L})$, i.e. the least common multiple of the minimal annihilators $f_a(T) \in \mathbb{Z}_p[T]$ of all elements $a \in L(A)$. For $x \in M$ the order is naturally defined by $\text{ord}(x) = \min\{p^k : p^k x = 0\}$ and the *essential order* is $\text{ess.ord}(x) = \text{ord}(T^j x)$ for all but possibly finitely many $j \geq 0$. If $\psi : M \rightarrow \mathcal{E}(M)$ is a pseudoisomorphism, then $\text{ess.ord}(x) = \text{ord}(\psi(x))$, since $\mathcal{E}(M)$ has no finite submodules.

Lemma 1. *Let $x \in M$ and $p^k = \text{ord}(x)$, $p \leq p^l = \text{ess.ord}(x) \leq \text{ord}(x)$. Then for any $g \in \Lambda$ we have $gx = 0 \Rightarrow g \equiv 0 \pmod{p^l}$ and there is a distinguished polynomial $G(T) \in \mathbb{Z}_p[T]$ such that $G(T)A \subset M$, while $\text{ord}(y) = \text{ess.ord}(y)$ for all $y \in G(T)A$.*

If $x \in A \setminus D$ and $p^{\delta(x)}x = c + z, c \in L, z \in M$, where $\delta(x)$ is the order defined in (2), then $c \notin pL$.

Proof. We fix a pseudoisomorphism $\psi : M \rightarrow \mathcal{E}(M)$. By definition of the essential order, $p^l = \text{ess.ord}(\psi(x))$ and if $g(T)x = 0$ then $\psi(g(T)x) = g(T)\psi(x) = 0$ thus $g(T) \equiv 0 \pmod{\text{ess.ord}(x)}$, as claimed.

We show the existence of $G(T)$ in two steps. First, if $F(T)$ is a distinguished polynomial that annihilates L , then $F(T)A \subset M$. If $g(T)$ is a distinguished polynomial that annihilates $\text{Ker}(\psi) = F(A)$, then the restriction $\psi : g(T)M \hookrightarrow \mathcal{E}(M)$ is injective, so $\text{ord}(y) = \text{ess.ord}(y)$ for all $y \in gM$. We may thus choose $G(T) = F(T)g(T)$ as a polynomial satisfying the second claim of the lemma.

Let now $x \in A \setminus D$ and assume the final claim is false, so $p^{\delta(x)}x = c + u = p\gamma + u, \gamma \in L$. Let $y := p^{\delta(x)-1}x$. Then $p(y - \gamma) = u \in M$ and it follows that $u' := y - \gamma \in M$ too. But then $p^{\delta(x)-1}x = y = \gamma + u' \in D$, in contradiction with the minimality of δ . The hypothesis $c \in pL$ was thus false, which completes the proof of the lemma. \square

We introduce the distances $d_n : A \times A \rightarrow \mathbb{N}$ as follows: let $x, z \in A$; then

$$d_n(x, z) := p\text{-rk}(\Lambda(x_n - z_n)); \quad d_n(x) = p\text{-rk}(\Lambda x_n).$$

We obviously have $d_n(x, z) \leq d_n(x, y) + d_n(x, z)$ and $d_n(x) \geq 0$ with $d_n(x) = 0, \forall n > 0$, for the trivial module. Also, if $f \in \mathbb{Z}_p[T]$ is some distinguished polynomial of degree $\phi = \deg(f)$, then $d_n(x) - \phi \leq d_n(fx) \leq d_n(x)$ for all $x \in A$. We shall write $d(x, y) = \lim_n d_n(x, y)$. We may also write $d(u, v) = p\text{-rk}(\Lambda(u - v))$ if $u, v \in A_k$, but we know no lifts of u and/or v to A : the difference consists here in the fact, that u, v appear as individual elements of A_k , rather than elements of a given norm coherent sequence. The simplest fact about the distance is

Fact 1. *Let $x, z \in A$ be such that $d_n(x, z) \leq N$ for some fixed bound N and all $n > 0$. Then $x - z \in L$ and $N \leq \ell := p\text{-rk}(L)$. For every fixed $d \geq 2p\text{-rk}(L)$ there is an integer $n_0(d)$ such that for any $x \in A \setminus L$ and $n > n_0$, if $d_n(x) \leq d$ then $x \in \nu_{n, n_0}A + F$.*

Proof. The element $y = x - z$ generates modules of bounded rank, so it is neither of μ -type nor indecomposed. Thus $y \in L$ and consequently $d_n(y) \leq p\text{-rk}(L_n) \leq \ell$ for all n , which confirms the claim.

For the second claim, note that if $x \notin L$, then $d_n(x) \rightarrow \infty$, so the boundedness of $d_n(x)$ becomes a strong constraint for large n . Next we recall that $F(T)x \in M$ and since $d_n(F(T)x) \leq d_n(x)$, we may assume that $x \in M$. Now $d_n(x) \leq d$ implies the existence of some distinguished polynomial $h \in \mathbb{Z}_p[T]$ with $\deg(h) = d$ and such that $h(T)x_n = 0$. The exponent of M is uniformly bounded by p^B , as a consequence of the Theorem of Babaicev – Monsky, so there is a finite set $\mathcal{H} \subset \mathbb{Z}_p[T]$ from which h can take its values. Let now n_0 be chosen such that $\nu_{n_0, 1} \in (h(T), p^B)$ for all $h \in \mathcal{H}$. Since m depends on \mathbb{K} , it follows that n_0 only depends on \mathbb{K} too. Then $h(T)x_n = 0$ implies $\nu_{n_0, 1}(x_n) = 0$ and thus, by Iwasawa's Theorem 6 (see also (4) and Lemma 3 below) there is a $z \in A$ such that $\nu_{n_0, 1}(x) = \nu_{n, 1}(z)$. Consequently $\nu_{n_0, 1}(x - \nu_{n, n_0}z) = 0$ and thus $x = \nu_{n, n_0}(z) + y$ for some y and the claim follows if we show that $y := x - \nu_{n, n_0}(z) \in F$. Since $\nu_{n_0, 1}y = 0$, it follows that $y \in L$ and the result of Sands in Lemma 14 in the Appendix implies that Λy must be finite, so $y \in F$, as claimed.

We now show that for fixed $h \in \mathcal{H}$ there is some even m such that $\nu_{m, 1} \in (h, p^\mu)$. Let the Euclidean division yield

$$\nu_{m, 1} = q_m(T)h(T) + r_m(T),$$

and let $\xi_i \in \overline{\mathbb{Q}_p}$ be the zeroes of h . Then

$$r_m(\xi_i) = \nu_{m, 1}(\xi_i) = \frac{(1 + \xi_i)^{p^m} - 1}{\xi_i} = O(p^{m/2}) + O(\xi_i^{p^{m/2}}).$$

Since \mathcal{H} is finite, there is some lower bound δ with $v_p(\xi_i) \geq \delta$ and the above identity shows that $v_p(r_m) \rightarrow \infty$ with diverging m , so one can choose m sufficiently large, such that $v_p(r_m) > \mu$ and thus $r_m \equiv 0 \pmod{p^\mu}$, so

$\nu_{m,1} \in (h(T), p^\mu)$. This can be achieved for all $h \in \mathcal{H}(T)$ and the claim is satisfied by choosing $n_0 = \max_{h \in \mathcal{H}}(m(h))$. \square

The arguments of this chapter will take repeatedly advantage of the following elementary Lemma³:

Lemma 2. *Let A and B be finitely generated abelian p -groups denoted additively, and let $N : B \rightarrow A$, $\iota : A \rightarrow B$ be two \mathbb{Z}_p -linear maps such that:*

1. *N is surjective.*
2. *The p -ranks of A and B are both equal to r and $|B|/|A| = p^r$.*
3. *$N(\iota(a)) = pa, \forall a \in A$.*

Then

- A. *The inclusion $\iota(A) \subset pB$ holds unconditionally.*
- B. *Suppose that $\text{sexp}(A) > p$. Then $p\text{-rk}(A) = p\text{-rk}(\iota(A))$ (i.e. ι is rank-preserving) and $\iota(A) = pB$, while $B[p] = \text{Ker}(N) \subset \iota(A)$. Moreover, $\text{ord}(x) = p \cdot \text{ord}(\iota(Nx))$ for all $x \in B$.*
- C. *If $\text{sexp}(A) > p$ and there is a group homomorphism $T : B \rightarrow B$ with $\iota(A) \subseteq \text{Ker}(T)$ and $\nu := \iota \circ N = p + \binom{p}{2}T + O(T^2)$, then $\nu = \cdot p$, i.e. $\iota(N(x)) = px$ for all $x \in B$.*

Proof. Since A and B have the same p -rank and N is surjective, we know that the map $\overline{N} : B/pB \rightarrow A/pA$ is an isomorphism⁴. Therefore, the map induced by $N\iota$ on the roof is trivial. Hence $\bar{\iota} : A/pA \rightarrow B/pB$ is also zero and thus $\iota(A) \subset pB$. This confirms the claim A.

We now consider the map $\iota' : A/pA \rightarrow pB/p^2B$ together with \overline{N} . From the hypotheses we know that $N\iota'$ is the multiplication by p isomorphism: $\cdot p : A/pA \rightarrow pA/p^2A$, using the fact that $\text{sexp}(A) > p$ which implies that $p\text{-rk}(A) = p\text{-rk}(\iota(A))$. It follows that ι' is an isomorphism of \mathbb{F}_p -vector spaces and hence $\iota : A \rightarrow pB$ is surjective. From $|B| = p^r|A| = p^r|pB|$ we see that $|A| = |pB|$ and thus $\iota : A \rightarrow pB$ is an isomorphism; it is in particular rank preserving. The cokernel of ι is an \mathbb{F}_p -vector space of dimension r .

Taking Pontrjagin duals, the roles of N and ι are interchanged. Hence the statement about cokernel of ι implies that the kernel of N is also annihilated by p and has order p^r ; it thus coincides with $B[p]$ and since ι is rank preserving, it follows that $B[p] = \iota(A)[p] \subset \iota(A)$. Let now $x \in B \setminus pB$ have order qp and let $r = \text{ord}(\iota(Nx))$. Then $N(rx) = rN(x) = 0$, so $rx \in \text{Ker}(N) = B[p]$ and $rp x = 0$, thus $q|r$. Conversely, $qx \in B[p] = \text{Ker}(N)$, so $\iota(qN(x)) = \iota(N(qx)) = 0$, implying $r|q$. Therefore $q = r = \text{ord}(\iota(Nx)) = \text{ord}(x)/p$, which completes the proof of point B.

For point C. we let $x \in B$, so $px \in pB = \iota(A)$ and thus $Tpx = pTx = 0$. Consequently $Tx \in B[p] \subset \iota(A)$ and therefore $T^2x = 0$. From the definition

³I owe the proof of the Lemma to Cornelius Greither, who provided an elegant simplification of my original proof.

⁴For finite abelian p -groups X we denote $R(X) = X/pX$ by *roof* of X and $S(X) = X[p]$ is its *socle*.

of $\nu = p + Tp\frac{p-1}{2} + O(T^2)$ we conclude that $\nu x = px + \frac{p-1}{2}Tpx + O(T^2)x = px$, which confirms the claim C. and completes the proof. \square

2.1. Kummer extensions, Property F and stabilization. Iwasawa has proved in his classical Theorem 6 from [8] a property relating ramification to the first cohomology of the groups $A(\mathbb{L}_n)$. We review here his construction, which shall be generalized for our context; we refer the reader either to the original paper [8], or the Lemmata 13.14-13.16 in [17]. Let $\{\mathfrak{P}_i : i = 1, 2, \dots, s\} \subset \mathbb{H}$ be a set of primes above the unique primes $\wp_i \subset \mathbb{K}; i = 1, 2, \dots, s$ above p , which ramify completely in \mathbb{L}/\mathbb{K} . Since \mathbb{H}/\mathbb{L} is unramified, it follows that the inertia groups $I(\mathfrak{P}_i) \subset \text{Gal}(\mathbb{H}/\mathbb{K}) \cong \Gamma$ are all isomorphic to \mathbb{Z}_p and one can choose topological generators $\tau_i \in I(\mathfrak{P}_i)$ which restrict to a fixed topological generator $\tau = \tau_i|_{\mathbb{L}} \in \text{Gal}(\mathbb{L}/\mathbb{K})$. Following Iwasawa [8], we let $a_i \in A$ be such that $\tau_i = \varphi(a_i)\tau_1, i = 2, 3, \dots, s$ and identify a lift of τ to $\text{Gal}(\mathbb{H}/\mathbb{K})$ with τ_1 . Let $Y = \bigoplus_{i=2}^s \mathbb{Z}_p\varphi(a_i) \subset X$ and $Y_n = \omega_n X + \nu_{n,1}Y = \nu_{n,1}(Y + TX)$. Then Iwasawa's Theorem 6 in [8] states that

$$(4) \quad A_n \cong X/Y_n, \quad Y_n = \omega_n X + \nu_{n,1}Y = \nu_{n,1}(Y + TX) \quad \forall n,$$

and thus $a \in A$ has $a_n = 0$ iff $a \in \varphi^{-1}(Y_n)$. In view of the Lemma 14 in the Appendix, one verifies that (4) is equivalent to

$$(5) \quad H^1(\Gamma|_{\mathbb{L}_n}, A_n) \cong Y_n/\omega_n X \cong Y/(Y \cap TX),$$

the last isomorphism holding only for large enough n . If $Y \subset TX$, or, equivalently, $H^1(\Gamma|_{\mathbb{L}_n}, A_n) = 0$ for all $n > 1$, we say that $A(\mathbb{L})$ has *Property F^5* , or simply that \mathbb{L}/\mathbb{K} has this property.

We retain the above facts for future reference:

Lemma 3. *Let \mathbb{L}/\mathbb{K} be a \mathbb{Z}_p -extension in which all the primes above p ramify completely, let Λ be the associated Iwasawa algebra and $\Gamma = \text{Gal}(\mathbb{L}/\mathbb{K}), X = \text{Gal}(\mathbb{H}/\mathbb{L})$. There is a finitely generated \mathbb{Z}_p -module $Y \subset X$ such that (4) and (5) hold for every $n > 0$. Moreover, $Y \not\subset TX$ iff there is some $y \in A \setminus TA$ with $y_1 = 0$.*

We shall be concerned with various phenomena of module stabilization, for which we start by introducing

Definition 4. *Let $\mathbb{L} \subset \mathbb{F} \subset \mathbb{H}$ be a galois extension of \mathbb{K} , let the intermediate fields be $\mathbb{F}_n = \mathbb{F} \cap \mathbb{H}_n, \overline{\mathbb{F}}_n = \mathbb{F}_n \cdot \mathbb{L}$, let $X_n = \text{Gal}(\overline{\mathbb{F}}_n/\mathbb{L})$ and $X = \varprojlim_{n \geq 0} X_n$. Let $F = F(X), L = L(X), M = M(X)$ be the modules in Definition 3, associated to X .*

If $F' \subset F$, we say that F'_n is stable, if $F'_m \cong F'_n \cong F'$ for all $m \geq n$. If $L' \subset L$ then L'_n is stable if $p\text{-rk}(L'_n) = p\text{-rk}(L'_m) = p\text{-rk}(L')$. Let $Y_n := H^0(\text{Gal}(\mathbb{L}_n/\mathbb{K}), A_n)$. We say that the H -part is stable (for $m > n$) if

$$Y_n \cong Y_{n-1} \cong Y(\mathbb{F})/TX \quad \text{for all } m > n.$$

⁵The name recalls Furtwängler, who first noted this property in a slightly different context of class field theory.

The smallest integer $v > 0$ such that $x_v \neq 0$ for all $x \in A(\mathbb{L}) \setminus \mathfrak{M}A(\mathbb{L})$ is called the visibility index; more general, if $C \subset A(\mathbb{L})$ and $I \subset \Lambda$ is an ideal, the visibility index of C with respect to I is $v := \min_k \{k : x_k \neq 0, \forall x \in C \setminus IC\}$.

The least integer n_0 for which F, L, H and M are stable is the stabilization index of X . It will be useful to assume that the stabilization index additionally fulfills the condition $x_0 \neq 0$ for all $x \in X \setminus IX$. Unless otherwise specified, the ideal $I = \mathfrak{M}$.

Stabilization criteria for the module A were first given by Fukuda [6], in the case when $\mu(\mathbb{L}) = 0$. S. Kleine has studied in his Thesis a large spectrum of stabilization conditions in multiple Λ -extensions. The result we present here is a variant of the statements proved by him.

Proposition 1. *Let \mathbb{L}/\mathbb{K} be a \mathbb{Z}_p -extension in which the primes above p are totally ramified and let $\mathbb{L} \subset \mathbb{F} \subset \mathbb{H}$ be a galois extension of \mathbb{K} with group $X = \text{Gal}(\mathbb{F}/\mathbb{L})$. Then*

1. *If $X_n \cong X_{n+1} \neq 0$ for some $n > 0$, then $X_n \cong X$ and X is finite.*
2. *If $p\text{-rk}(X_n) = p\text{-rk}(X_{n+1}) > 0$ for some $n > 0$, then $p\text{-rk}(X_n) = p\text{-rk}(X)$ and $\mu(X) = 0$.*
3. *Let $V_n := X_n/TX_n$; if $V_n \cong V_{n+1} \neq 0$ then $V_n \cong X/TX$ and $Y_n/TX_n \cong Y/TX$, the H -part being stable for $m > n$ and $X[T]$ finite.*

Proof. Let $Y = Y(\mathbb{F})|_{\mathbb{F}}$ and $Y_n = \nu_{n,1}(Y + TX)$. We have proved that $X_n \cong X/Y_n$ and assume without restriction of generality that 1 is the least integer n for first stabilization in both cases 1. and 2. We have the following commutative diagram in which $X_n \rightarrow X_1$ is induced by the map $\nu_{n,1}$ while the horizontal isomorphisms are deduced from the definition of Y_n .

$$(6) \quad \begin{array}{ccc} X_n & \cong & X/\nu_{n,1}Y \\ \downarrow & & \downarrow \\ X_1 & \cong & X/Y. \end{array}$$

For the first point we assume $|X_2| = |X_1|$. Then $X_2 \rightarrow X_1$ is an isomorphism; therefore $\nu_{2,1}Y = Y$. Since $\mathfrak{M} = (p, T) \subset \Lambda$ is the unique maximal ideal and $\nu_{2,1} \in \mathfrak{M}$, and since Y is finitely generated over Λ , it follows from Nakayama's lemma that $Y = 0$. Consequently, $X \cong X_1$ and $X_n \cong X_1 \cong X$ for all $n \geq 1$. The condition $X_2 \cong X_1$ readily implies finiteness of the X , which proves the assertion 1.

Suppose now that $p\text{-rk}(X_2) = p\text{-rk}(X_1)$. Then $X_2/pX_2 \cong X_1/pX_1$ and thus $X/(\nu_{2,1}Y + pX) \cong X/(Y + pX)$ and $\nu_{2,1}Y + pX \cong Y + pX$. Letting $Z = (Y + pX)/pX$, we have

$$\nu_{2,1}Z = (\nu_{2,1}Y + pX)/pX = (Y + pX)/pX = Z.$$

By Nakayama's lemma, we conclude that $Z = 0$ and $Y \subset pX$. Therefore,

$$\begin{aligned} p\text{-rk}(X_n) &= p\text{-rk}(X/\nu_{n,1}Y) = p\text{-rk}(X/(\nu_{n,1}Y + pX)) \\ &= p\text{-rk}(X/pX) = \mathbb{Z}_p\text{-rk}(X), \quad \text{for all } n \geq 0. \end{aligned}$$

By Iwasawa's formula, for n sufficiently large we have

$$|X_n| = p^{\mu p^n + \lambda n + \nu},$$

and since the rank stabilizes, we see that $\mu(X) = 0$ and $|X_{n+1}|/|X_n| \geq p^\lambda$ with equality iff $F(X) = 0$. In this case too, $\mu(X) = 0$ is a consequence of the stabilization condition. This proves assertion 2.

Finally the stabilization of the cohomology part is analogous to point 1. We have $V_n = X_n/TX_n = X/(TX + \nu_{n,1}Y)$. Let $W_n = \nu_{n,1}Y$ so $TX + \nu_{n,1}Y_n = TX + W_n$ while $TX + \nu_{n+1,1}Y = TX + \nu_{n+1,n}W_n$. In exact sequences

$$(7) \quad \begin{array}{ccccccc} 0 & \rightarrow & TX + W_n & \rightarrow & X & \rightarrow & X/(TX + W_n) \rightarrow 0 \\ 0 & \rightarrow & TX + W_{n+1} & \rightarrow & X & \rightarrow & X/(TX + W_{n+1}) \rightarrow 0, \end{array}$$

the isomorphism $V_{n+1} = X/(TX + W_{n+1}) \cong X/(TX + W_n) = V_n$ implies that $TX + W_n \cong TX + \nu_{n+1,n}W_n$. It follows from Nakayama's Lemma that $W_n \subset TX$; indeed, the module $Z_n := TX + W_n$ is finitely generated, so let $t_1, t_2, \dots, t_r \in TX \setminus \mathfrak{M}TX$ be a minimal set of generators of TX . Assuming that $TX \neq Z_n$ there is a minimal set of generators $w_1, w_2, \dots, w_j \in W_n \setminus (\mathfrak{M}Z_n + TX)$ such that $(W_n + TX)/TX = \sum_j \Lambda \bar{w}_j$. But since $TX + W_n = TX + \nu_{n+1,n}W_n$, we deduce that $\sum_j \Lambda \bar{w}_j = \nu_{n+1,n} \sum_j \Lambda \bar{w}_j$ and since $\nu_{n+1,n} \in \mathfrak{M}$ it follows that $(TX + W_n)/TX = 0$, and $\nu_{n,1}Y \subset TX$. A fortiori $\nu_{m,1}Y \subset TX$ and thus $Z_m = X/TX$ for all $m > n$. It follows in particular that X/TX is finite and since $|X/TX| = |X_n/TX_n| = |X_n[T]|$ for sufficiently large n , it follows that $H^0(\text{Gal}(\mathbb{L}_n/\mathbb{K}), A_m)$ is stable for $m > n$. \square

The strength of this Fukuda-type result is that it shows that the first stabilization occurring within the projective sequence of galois groups X_n readily implies global stabilization.

The stabilization conditions above require no a priori knowledge about the shape of X . Moreover, if H is stable, then all $x \in A \setminus \mathfrak{M}A$ are visible. It is however not possible to determine stabilization of μ -parts from internal data, as the following example shows:

Example 1. Let $\mathbb{K} = \mathbb{Q}[\sqrt{-d}]$ be an imaginary quadratic field with trivial p -part of the class field and let \mathbb{K}_∞ be its cyclotomic \mathbb{Z}_p -extension. For $n > 0$ we consider a principal prime ideal $\mathfrak{q} = (\gamma_n) \subset \mathbb{K}_n$, which is totally split over \mathbb{Q} and also splits in $\mathbb{K}[\zeta_p]$. If $q \in \mathbb{N}$ is the rational prime above it, then $q \equiv 1 \pmod{p}$ and we let $\mathbb{F} \subset \mathbb{Q}[\zeta_q]$ be the subfield of degree p while $\mathbb{L} = \mathbb{K} \cdot \mathbb{F}$.

Then it can be shown (see next chapter), that there is an ideal $\mathfrak{R} \subset \mathbb{L}_n = \mathbb{K}_n \cdot \mathbb{F}$ with class $r_n = [\mathfrak{R}/\overline{\mathfrak{R}}]$ and such that $\mathbf{N}_{\mathbb{L}/\mathbb{K}}(r_n) = 1$, while $\Lambda r_n \cong \Lambda/(p, \omega_n)$. Assuming that $A^-(\mathbb{L}) = \Lambda r$ for a norm coherent sequence containing r_n , we see that $A^-(\mathbb{L})$ has μ -like growth up to level n , but since $\mu(\mathbb{L}) = 0$ by the Theorem of Ferrero-Washington, the p -rank of Λr_m must stabilize for some $m > n$. This fact cannot be detected by analyzing the sequence r_1, r_2, \dots, r_n .

Of course, rank stabilization eventually takes place in this example, so it can be detected by Proposition 1. Therefore it would be interesting to know whether, in the case when $\mu > 0$, the rank stabilization of some submodule can be perceived. A partial answer is contained in Proposition 1, which allows choosing subfields of the Hilbert class field – so the question is transformed into one of constructing an adequate subfield.

We now give some applications of the Fukuda result. We keep the same notation for $\mathbb{K} \subset \mathbb{L} \subset \mathbb{F} \subset \mathbb{H}' \subset \mathbb{H}$, with \mathbb{H}' being the maximal subextension of \mathbb{H} which splits all the primes above p .

We let $\mathbb{H}^{(l)} = \mathbb{H}^{\varphi(M)}$, where $M = A^\circ$ and $\mathbb{H}^{(t)} = \mathbb{H}^{T\varphi(A)}$, the indicator for stabilization of H -parts. The galois groups are

$$X = \text{Gal}(\mathbb{H}/\mathbb{L}), \quad X^{(x)} = \text{Gal}(\mathbb{H}^{(x)}/\mathbb{L}), \quad x \in \{l, t\}.$$

The Proposition 1 can be applied to these extensions in order to establish the stabilization index n_0 of \mathbb{L} . As a direct consequence we have

Fact 2. *Let $x \in X^{(l)}$; for n beyond the stabilization index n_l of $X^{(l)}$ and for all $k > 0$, we have $\iota_{n,n+k}(x_n) = p^k x_{n+k}$.*

Proof. The choice of n_l implies that $p\text{-rk}(X_n^{(l)}) = p\text{-rk}(X_{n+1}^{(l)}) = p\text{-rk}(X^{(l)})$. For $k = 1$, we let $B = X_{n+1}^{(l)}$ and $A = X_n^{(l)}$. Then N, ι are the restriction $N_{\mathbb{K}_{n+1}, \mathbb{K}_n}$ and the lift map. The choice of n also implies that $\text{sexp}(A) > p$ and we let $T = \omega_n$ in Lemma 2. We deduce from point C that

$$(8) \quad \iota x_n = p x_{n+1},$$

which is the statement for $k = 1$. The general case follows by induction on k , letting $A = X_{n+i}^{(l)}, B = X_{n+i+1}^{(l)}$ for $i = 0, 1, \dots, k-1$, successively, and applying the result for $k = 1$ established previously. Indeed, assume that for all $j \leq i$ we have $\iota_{n,n+i}(x_n) = p^i x_{n+i}$. Using also the fact that $\iota_{n+i,n+i+1}(x_{n+i}) = p x_{n+i+1}$ which follows from (8), we find

$$\begin{aligned} \iota_{n,n+i+1}(x_n) &= \iota_{n+i,n+i+1}(\iota_{n,n+i}(x_n)) = \iota_{n+i,n+i+1}(p^i x_{n+i}) \\ &= p^{i+1} x_{n+i+1}, \end{aligned}$$

and thus it follows by induction that $\iota_{n,n+i}(x_n) = p^i x_{n+i}$ and the claim follows by letting $i = k$. \square

2.2. Decomposition. We let \mathbb{L}/\mathbb{K} be some \mathbb{Z}_p -extension in which all the primes above p are totally ramified and p^B be the exponent of A° . We let $n_0 > 0$ be an index such that

$$(9) \quad \text{sexp}(L_{n_0}) \geq p^4 \quad \text{and} \quad p\text{-rk}(L_n) = p\text{-rk}(L_{n_0}) \quad \forall n \geq n_0.$$

Note that the condition (9) is fulfilled by all submodules $L' \subset L$ which are spanned by elements of infinite order – or such ones of order at least p^4 . We assume, without loss of generality, that this is the case for L too. We note the following

Fact 3. *With the notations of this section, for all $n > n_0$ and all $x = (x_n)_{n \in \mathbb{N}} \in L$, we have*

$$L_{n+2}[p^2] \subset \iota_{n,n+2}(L_n) \quad \text{and} \quad \omega_n \cdot \omega_{n_0}(x_{n+1}) = 0.$$

Proof. By hypothesis, we have $\text{sexp}(L_n) \geq p^4$; since $\exp(\text{Ker}(\iota_{n,n+2} : L_n \rightarrow L_{n+2})) = p^2$, it follows that $\text{sexp}(\iota_{n,n+2}(L_n)) \geq p^2$. The ranks are conserved, by hypothesis, so we conclude that $\iota_{n,n+2}(L_n) \supset L_{n+2}[p^2]$. For arbitrary $n \geq n_0$ we have $px_{n+1} = \iota_{n,n+1}(x_n)$ and thus $\omega_n x_{n+1} \in L_{n+1}[p]$. The second fact will now be proved by induction on n .

For $n = n_0$ we have $\omega_n x_{n+1} \in L_{n+1}[p] \subset \iota(L_{n_0})$, and thus $\omega_n \omega_{n_0}(x_{n+1}) = 0$. Let now $n > n_0$ be fixed and assume that $\omega_n \omega_{n_0}(x_{n+1}) = 0$. Using

$$\omega_{n+1} = \omega_n \cdot \nu_{n+1,n} = \omega_n \cdot (pu(\omega_n) + \omega_n^{p-1}),$$

we conclude that

$$\begin{aligned} \omega_{n_0} \omega_{n+1}(x_{n+2}) &= \omega_{n_0} \omega_n pu(\omega_n)(x_{n+2}) + \omega_{n_0} \omega_n^p(x_{n+2}) \\ &= \iota_{n+1,n+2}(\omega_{n_0} \omega_n(x_{n+1})u(\omega_n)) + \omega_{n_0} \omega_n^p(x_{n+2}) = \omega_{n_0} \omega_n^p(x_{n+2}) \end{aligned}$$

where the last equality follows from the induction hypothesis. Now $p^2 \omega_n x_{n+2} = \iota_{n,n+2}(\omega_n x_n) = 0$, hence $\omega_n x_{n+2} \in L_{n+2}[p^2] \subset \iota_{n,n+2}(L_n)$ and thus $\omega_n^2 x_{n+2} = 0$, which completes the proof. \square

We let B be an upper bound for $v_p(\mu)$ over the μ invariants of all \mathbb{Z}_p -extensions of \mathbb{K} , so p^B is a safe upper bound for $\exp(M(\mathbb{L})/F(\mathbb{L}))$. We let $F(T) \in \Lambda$ be the minimal annihilator polynomial of $L(A)$ and note that $\mathbf{D} := A/D$ is a finite Λ -module. We shall also assume, without restriction of generality, that $n_0 = 1$ for our base field \mathbb{K} : this can be achieved by a shift up of the base field.

Passing to decomposition, we note the following property:

Lemma 4. *Let \mathbb{L}/\mathbb{K} be a \mathbb{Z}_p -extension satisfying the condition (9) and let the further notations be as defined above. The modules D, M, L, F are defined with respect to A . If $px \in D$ then $T^2x, \omega_2x \in D$.*

Moreover, if $x \notin D$ but $px, Tx \in D$ and $Tx = x_\lambda + x_\mu$, then $\text{ord}(x_{\mu,1}) = p$ and $x_{\mu,1} = -x_{\lambda,1}$.

Proof. Let $w \in A \setminus (\mathfrak{M}A + D)$ and suppose that $l \leq B$ is the smallest integer such that $p^l w \in L$ and let $f_w(T)$ be the minimal annihilator polynomial of $p^l w$. Then $y := f_w(T)w \in M$ and $p^l y = 0$. There is some $0 < d \leq l \leq B$ such that $x := p^{d-1}w$ verifies $x \notin D$ but $px \in D$; note that l, d are the orders introduced in (2). Let $\mathcal{X} = \{x \in A \setminus D : px \in D\} \subset A$ and $\mathcal{X}' \subseteq \mathcal{X}$ be the set of those elements that arise as described above. Then

$$p^j x_{n+j} - \iota_{n,n+j}(x_n) \in f_x(T)\Lambda x_{n+j} \subset \Lambda y_{n+j}, \quad \forall j > 0.$$

In particular $\iota_{n,n+l}(x_n) = p^l x_{n+l} - h_{n+l}(T)(f_x x_{n+l})$ is decomposed and for $n > n_0$ and $x \in A \setminus D$ such that $\text{ord}(p^l x_n) > p$, we have

$$(10) \quad p^l x_{n+l} - \iota_{n,n+l}(x_n) = f_x(T)h_n(T)x_{n+l} \in M_{n+l}.$$

Indeed, consider the modules $B = \Lambda x_{n+1}/(f_x \Lambda x_{n+1})$ and $A = \Lambda x_n/(f_x \Lambda x_n)$. Since $\iota_{n,n+1}(x_n) \notin f_x \Lambda x_{n+1}$ for $n > n_0$ – as follows from the condition imposed on the orders – the induced map $\iota : A \rightarrow B$ is rank preserving. We can thus apply the Lemma 2, which implies the claim (10), and deduce under the above hypothesis on n , that

$$p^l x_{n+l} = p^{l-1} c_{n+l} = \iota_{n+1,n+l}(c_{n+1}) = \iota_{n,n+l}(x_n) + h y_{n+l}, \quad h \in \mathbb{Z}_p[T].$$

By Fact 3 and the choice of \mathbb{K} such that $n_0 = 1$, we have $\omega_n T c_{n+1} = 0$. Applying ω_n to the above identity we find $Th \omega_n y_{n+l} = 0$. The relation (4) implies that there is some $z \in A$ such that $T^2 h \omega_n y = \omega_{n+l} z$. In addition, we have $p^l \omega_{n+l} z = 0$. The result of Sands of Lemma 14 yields $z \in M + A[T]$. Then $\omega_n(T^2 h y - \nu_{n,n+l} z) = 0$ implies $T^2 h y \in \nu_{n,n+l} z + A[T] + F$. Since $h y \in M$, it follows that $z \in M$ and $T^2 h y \in \nu_{n,n+l} z - \phi$, say, for some $\phi \in F$. Reinserting this relation in the initial identity, we find

$$(11) \quad \iota_{n,n+l}(T^2 x_n + z_n) = \iota_{n+1,n+l}(T^2 c_{n+1}) - \phi_{n+l}$$

Note that the right hand side is in L and thus has uniformly bounded p -rank. This leads to the following two proofs for the fact that (11) implies that $T^2 x$ must be decomposed. For the first, we invoke the Lemma 1 with respect to the sequence $w^{(n)} = T^2 x + z$, where the upper index stresses the fact that the choice of z depends on n . Since $d_n(\iota_{n+1,n+l}(T^2 c_{n+1})) \leq p\text{-rk}(L)$ for all n , the Lemma 1 implies that there is an uniform $n_0 > 0$ such that $w_n^{(n)} \in \nu_{n,n_0} A + F$. But then

$$w_n^{(n)} = \iota_{n,n+l}(T^2 x_n + z_n) = \nu_{n,n_0}(a_n + f_n) \in \iota_{n_0,n}(A_{n_0}).$$

It follows in particular that

$$\text{ord}(T^2 x_n + z_n) \leq p^l \text{ord}(\iota_{n,n+l}(T^2 x_n + z_n)) \leq p^l \exp(A_{n_0}).$$

This holds for arbitrary large n and since $z_n \in M$ we have $\text{ord}(T^2 x_n + z_n) = \text{ord}(T^2 x_n)$, thus obtaining a contradiction if $T^2 x_n \notin D$, case in which $\text{ord}(x_n) \rightarrow \infty$.

The second proof uses topological facts. If $f \in \mathbb{Z}_p[T]$ is the minimal annihilator polynomial of $p^m x$ and thus of c , then we found that for every n there is a $z = z^{(n)} \in M$ such that $f T^2 x_n + f z_n^{(n)} = 0$, thus

$$w_n := -T^2 y_n = f(T) z^{(n)}, \quad z^{(n)} \in M.$$

Let $m > n$; by definition, we have $w_m = f(T) z_m^{(m)}$ and, since $w = -T^2 y$ is a norm coherent sequence, a fortiori, $w_n = f(T) z_n^{(m)}$. We may assume that $z^{(m)} = z^{(n)}$ and therefore, upon extracting subsequences from the sequence $z^{(n)}$, the defining condition $w_n = f(T) z^{(n)}$ is conserved. Since M is a Noetherian module, we may choose a minimal system of generators $u^{(i)} \in M \setminus \mathfrak{M}M, i = 1, 2, \dots, s$ and let $z^{(n)} = \sum_{i=1}^s c_i^{(n)} u^{(i)}, c_i^{(n)} \in \Lambda$, where the representation is not unique. We obtain thus a sequence $(C_n)_{n \in \mathbb{N}}$ with $C_n = \left(c_i^{(n)} \right)_{i=1}^s \in \Lambda^s$. In the \mathfrak{M} -adic product topology, Λ^s is a compact

space. Letting $p^B M = 0$, we see that we may choose $c_i^{(n)} \in \mathbb{Z}_p[T]$ as polynomials with degree $\deg(c_i^{(n)}) \leq \deg \omega_n$ and coefficients of valuation at most B . There is a converging subsequence C_{n_i} . After eventual renumeration, we may thus assume that the sequence C_n is convergent. Let $C = (c_i)_{i=1}^s = \lim_n C_n$ and let for all n the polynomial $\omega_{n,B} \in \mathbb{Z}[T]$ have coefficients in $\{0, 1, \dots, p^B - 1\}$ and verify $\omega_{n,B} \equiv \omega_n \pmod{p^B}$. Note that the polynomials $c_i^{(n)}$ are all defined modulo $\omega_{n,B}$, while c_i is defined modulo p^B . After eventually extracting a new subsequence, we may assume that the C_n are such that

$$(12) \quad c_i^{(n)} - c_i \in \omega_{n,B} \Lambda, \quad \text{for all } n > 0 \text{ and } i = 1, 2, \dots, s.$$

Let $z = \lim_n z^{(n)} = \sum_i c_i u^{(i)}$. From $w_n = f(T)z^{(n)}$ we deduce that $w_n = \sum_i f(T)c_i^{(n)} u_n^{(i)}$ and since $c_i^{(n)} \equiv c_i \pmod{\omega_{n,B}}$ it follows that $w_n = \sum_i f(T)c_i u_n^{(i)} = f(T)z_n$. We have thus proved that $w = f(T)z$ for some $z \in M$ and thus $f(T)(z + T^2 x) = 0$, hence $z \in T^2 x + L$, which proves that $T^2 x \in D$ as claimed. Moreover, $\omega_2 = T(pu(T) + T^{p-2})$ and since px and $T^2 x \in D$ it follows also that $\omega_2 x \in D$, which completes the (second) proof of the first statement.

Suppose now that $Tx = x_\mu + x_\lambda$ and $px_\mu = x_{\mu,1} = 0$. Let $\mathcal{N} - p = psf_2(T) + s^{p-1}, f_2(T) \in \Lambda^\times$, and note that, in stable growth, $\omega_n x_{\lambda,n+1} \in L_{n+1}[p]$ and thus $\omega_n^2 x_{\lambda,n+1} = p\omega_n x_{\lambda,n+1} = 0$. Since $px_\mu = 0$, we have

$$\begin{aligned} -px_{n+1} + \iota_{n,n+1}x_n &= p\nu_{1,n}f_2(\omega_n)(x_{\lambda,n+1} + x_{\mu,n+1}) + \nu_{1,n}\omega_n^{p-2}(x_{\lambda,n+1} + x_{\mu,n+1}) \\ &= T^{D_n-1}x_{\mu,n+1}, \quad D_n = \deg(\omega_{n+1} - \omega_n) = \deg(\nu_{n,n+1}). \end{aligned}$$

Writing r_{n+1} for the right hand side in the above identities, we consequently obtain $\omega_n r_{n+1} = \nu_{n+1,1}x_{\mu,n+1} = x_{\mu,1} = 0$. By Lemma 3, there is thus some $z \in A$ such that $\omega_n r = \omega_n(\nu_{n+1,n} - p)x = \omega_{n+1}z$, so $r = \nu_{n,n+1}(z_{n+1})$ and consequently $\iota_{n,n+1}(x_{n+1} - z_{n+1}) = -px_{n+1} \in L_n$. However, we have seen that for $x \notin D$ and $y \in D$, the distance $d_n(x, y) \rightarrow \infty$; in particular the distance on the left hand side of the last identity will diverge, while the right hand side has upper bounded distance, since $px \in L$. This contradiction implies that for $x \in A \setminus D$ such that $px, Tx \in D$, we must have $x_{\mu,1} \neq 0$. Since $x_{\mu,1} + x_{\lambda,1} = Tx_1 = 0$, it follows that $x_{\mu,1} = -x_{\lambda,1}$. Since we assume that the growth of A is stable from the ground field, we have $\text{ord}(x_{\lambda,2}) = p\text{ord}(x_{\lambda,1}) = \text{ord}(Tx_2) = p$, thus $\text{ord}(x_{\lambda,1}) = \text{ord}(x_{\mu,1}) = p$, which completes the proof. \square

For individual \mathbb{Z}_p -extensions, we have:

Proposition 2. *Let \mathbb{L}/\mathbb{K} be a \mathbb{Z}_p -extension and A, Λ be associated to \mathbb{L} as usual. If p^B is the exponent of A° , then $\mathfrak{M}^{2B}A \subset D(A)$ and $\omega_B A \subset D(A)$.*

Proof. For $x \in A$ we let $k = \text{ord}_D(x) = \min\{j : p^j x \in D\}$ be the decomposition order of x . The proof will follow by induction on k , on base of the Lemma 4

For $k = 1$, it is a direct consequence of the lemma, since $\mathfrak{M}^2 = (p, pT, T^2)$. Assume that the statement holds for all $x \in A$ with $\text{ord}_L(x) < k$ and note that $\mathfrak{M}^{2k} = (p^2, pT, T^2)\mathfrak{M}^{2(k-1)}$. Since we assumed that $p^k x \in D$, it follows that px has order $k-1$ and by induction hypothesis, we have $p\mathfrak{M}^{2(k-1)}x \subset D$. For arbitrary $w \in \mathfrak{M}^{2(k-1)}x$ we have thus $pw \in D$ and the Lemma 4 implies that $T^2wx \in D$. The choice of w being free, it follows that $T^2\mathfrak{M}^{2(k-1)}x \subset D$ too, hence $\mathfrak{M}^{2k}x \subset D$. This holds for all k , and letting $k = m$ we conclude that $\mathfrak{M}^{2m}A \subset D$, which completes the proof. The fact $\omega_m A \subset D$ follows from Lemma 4 by induction too, the proof being similar. \square

As a consequence,

Corollary 1. *Let p^B be the exponent of M and suppose that $n' > n_0 + B$ with n_0 the stabilization index of \mathbb{L} ; if we shift the base field according to $\mathbb{K}_1 = \mathbb{K}_{n'}$ and redefine Λ accordingly, then $TA \subset D$.*

Proof. Let us write $\Lambda^{(0)}, T^{(0)}, \omega^{(0)}$, etc for the Iwasawa algebra and its elements, defined with respect to the initial base field $\mathbb{K}^{(0)}$, say. We have then $T = \omega_{n'}^{(0)}$. A simple computation shows that $\omega_n \in \mathfrak{M}^n$ for all n , so then $\omega_{n'}^{(0)} \in (\mathfrak{M}^{(0)})^{2B}$ and the claim follows from the Proposition 2. \square

The results above are indicative for what can be achieved in full generality. In our context, we shall need the following specific application for CM fields:

Lemma 5. *Let \mathbb{K}' be a CM galois extension of \mathbb{Q} containing the p -th roots of unity and let \mathbb{L}'/\mathbb{K}' be a \mathbb{Z}_p CM extension. The modules A, D, L, F are defined with respect to this extension and we consider $x \in A^-$ such that $px = c + v \in D^-$ with $c \in L^-, v \in M^-$, such that $\omega_n Tc_{n+1} = 0$ for all $n \geq 0$. Then $Tx \in D^-$.*

Proof. The proof is identical to the one of Lemma 4. Note the difference in premise: here we cannot make a global statement on the stability of L^- for all $n > 0$, but we do have sufficient information about the decomposition of px , so that the proof can be completed like in the proof of the Lemme 4, the details being left to the reader. \square

2.3. On CM \mathbb{Z}_p -extensions of number fields. In this section we gather several properties of CM \mathbb{Z}_p -extensions which are the base for our approach; recall that the occurrence of CM \mathbb{Z}_p -extensions different from the cyclotomic one, is *equivalent* to the failing of Leopoldt's conjecture for CM fields \mathbb{K} . We let \mathbb{K} be some galois CM number field for which the Leopoldt conjecture fails and let \mathbb{K}_∞ be its cyclotomic \mathbb{Z}_p -extension. We let \mathbb{M} be the compositum of all the \mathbb{Z}_p -extensions of \mathbb{K} , let \mathbb{M}_0^+ be the compositum of all the \mathbb{Z}_p -extensions of \mathbb{K}^+ and $\mathbb{M}^+ = \mathbb{K} \cdot \mathbb{M}_0^+ \subset \mathbb{M}$.

The radicals of \mathbb{M}^+ as a Kummer extension of \mathbb{K}_∞ are intimately related to the failure of Leopoldt's conjecture and the T^* -part of the class group, by the following *folklore* result, which holds in the cyclotomic \mathbb{Z}_p -extension of a field:

Proposition 3. *Let \mathbb{K} be a CM field which contains the p -th roots of unity and $A(\mathbb{K}) = \varprojlim_n A(\mathbb{K}_n)$ be defined with respect to the cyclotomic \mathbb{Z}_p -extension. Then*

$$\mathbb{Z}_p\text{-rk}(A^-[T^*]) = \mathcal{D}(\mathbb{K}),$$

and in particular Leopoldt's conjecture fails for \mathbb{K} iff $A^-[T^] \neq 0$. Moreover*

$$(13) \quad \mathbb{M}^+ \subseteq \mathbb{K}_\infty[(A^-(T^*))^{1/p^\infty}].$$

In particular, for every CM \mathbb{Z}_p -extension \mathbb{L}/\mathbb{K} there is a class $a \in A^-(T^) \setminus T^*A^-(T^*)$ such that $\mathbb{L} \cdot \mathbb{K}_\infty = \mathbb{K}_\infty[a^{1/p^\infty}]$.*

The proof of the proposition is given in the Appendix.

For the cyclotomic \mathbb{Z}_p -extension, it is known that $A^-(\mathbb{K}_\infty)$ has no finite p -torsion submodule. In the case of non-cyclotomic CM \mathbb{Z}_p -extensions, this fact is almost true, namely:

Lemma 6. *Let \mathbb{K} be a CM extension containing the p -th roots of unity and \mathbb{L}/\mathbb{K} be a CM \mathbb{Z}_p -extension with $\mathbb{L} \cap \mathbb{K}_\infty = \mathbb{K}_N, N > 1$ and write $\mathbb{L}_N := \mathbb{K}_N; [\mathbb{L}_{N+n} : \mathbb{K}_N] = p^n$. If $\mu_{p^N} \subset \mathbb{L}$ but $\mu_{p^{N+1}} \not\subset \mathbb{L}$ then the finite torsion submodule $C^- := F(A^-) \subset A^-$ is a cyclic group of order p^N . If $a = (a_n)_{n \in \mathbb{N}}$ is a generator of C^- , then*

$$(14) \quad \mathbb{L}_{N+m} = \mathbb{L}_{N+m-n}[a_{N+m-n}^{1/p^n}] \quad \text{for all } m, N \geq n,$$

with the root of a class defined like in Remark 1. Suppose that $T^ = T - p^k, 1 \leq k \leq N$ is the Iwasawa involution and assume that N is chosen such that*

$$(15) \quad p^{2k}a \neq 0 \quad \text{for all } a \in A_{N-1}^-(T^*) \subset pA_N^-(T^*).$$

*Then $T^*C^- = 0$.*

Proof. Let $c \in C^- \setminus pC^-$ generate a direct term of order $q := p^j; j \leq N$ in the abelian p -group C^- . Let $\mathfrak{C} \in c_m, m > N$ be a prime ideal. Since c is a finite torsion element, it follows that $\iota_{m,\infty}(c_m) = 0$, so we may assume that $l \geq j$ is the least integer such that $\iota_{m,m+l}(c_m) = 0$. In the sequel we show that we must in fact have $l = j$. Let $\mathfrak{C}^q = (d)$ and $\iota_{m,m+l}(\mathfrak{C}) = (\delta)$. Since \mathbb{L} is CM, we conclude from Kronecker's unit Theorem, after eventually modifying δ by some root of unity, that

$$\delta/\bar{\delta} = (d/\bar{d})^q.$$

We can thus apply Kummer theory in the abelian cyclic extension $\mathbb{L}_{l+m}/\mathbb{L}_m$. The minimality of l implies that $\delta/\bar{\delta} \notin ((\mathbb{L}_{m+l-1})^\times)^q$. By an inductive repetition of the argument, it follows that $\text{ord}(\iota_{m,m+l-j}(c_m)) = \text{ord}(c_m)$ and $\iota_{m,m+l-j}(\mathbb{Z}c_m) \cong \mathbb{Z}c_m$; thus

$$(16) \quad \mathbb{L}_{m+l} = \mathbb{K}_{m+j-l}[(d/\bar{d})^{1/q}] = \mathbb{L}_{m+l-k}[c_m^{1/q}].$$

This implies $j = l$; according to point B in the Remark 1, there is a class $a_m \in A_m^-$ of order $\text{ord}(a_m) = p^j$, such that $\mathbb{L}_{m+j} = \mathbb{L}_m[a_m^{1/p^j}]$. One verifies by using the same computations as above, that $\iota_{m,m+N}(a_m) = 0$. Taking a

norm coherent sequence $a = (a_i)_{i \in \mathbb{N}}$ through a_m , we see that $\text{ord}(a) \geq p^N$. Together with the inequality $j \leq N$, we conclude that $\exp(C^-) = p^N$. Moreover, we have shown that there is a sequence $a = (a_m)_{m \in \mathbb{N}} \in C^-$ with $\text{ord}(a) = p^N$ and $\mathbb{L}_{m+N} = \mathbb{L}_m[a_m^{1/p^N}]$ for all (sufficiently large) m .

We claim that C^- is \mathbb{Z}_p -cyclic, so $C^- = \mathbb{Z}a$. Since C^- is a

finite abelian p -group, we have $p\text{-rk}(C^-) = \dim_{\mathbb{F}_p}(C^-[p]) = \dim_{\mathbb{F}_p}(C^-/pC^-)$. We show that $C[p] \cong \mathbb{F}_p$, and thus $p\text{-rk}(C^-) = 1$. Let m be fixed and $c_m \in C_m[p]$ be a class, the primes of which become principal in \mathbb{L}_{m+1} . If $\mathfrak{C} \in c_m$ is a prime, $(\gamma) = \mathfrak{C}^p$ and $(\delta) = \iota_{m,m+1}(\mathfrak{C})$, then we showed that we may assume $\gamma^{1-j} = \delta^{p(1-j)}$. On the other hand, we have shown above that the sequence a can be chosen such that $\mathbb{L}_{m+N} = \mathbb{L}_m[a_m^{1/p^N}]$ and in particular $\mathbb{L}_{m+1} = \mathbb{L}_m[a_m^{1/p}]$. Concretely, let $(\gamma) = \mathfrak{A}_m^{p^N}$, $\mathfrak{A}_m \in a_m$. Then Kummer theory implies that there is an integer v , coprime to p , such that

$$\frac{\alpha}{\bar{\alpha}} = \left(\frac{\gamma}{\bar{\gamma}} \right)^v \cdot w^p, \quad w \in \mathbb{L}_m^\times.$$

Then $(\mathfrak{C}/\mathfrak{A}_m^{vp^{N-1}})^{1-j} = (w)$ and, in terms of classes, we conclude that $c_m = a_m^{vp^{N-1}}$. Since c_m was chosen arbitrarily, it follows that a_m generates C_m^- and thus $C^- = \mathbb{Z}a$ is a cyclic p -group of order p^N .

Finally, $T^*C^- = 0$ follows from the Proposition 3. Indeed, we have $\mathbb{L}_{2N} = \mathbb{L}_N[a_N^{1/p^N}]$ and the proposition implies that $a_N \in A_N[T^*]$, with $T^* = T - p^k$ for some fixed $k < N$, which depends on the choice of \mathbb{K} . Since the annihilator polynomial $f_a(T)$ is linear, say $f - a = T - vp^j$ and $T^*a_N = f_a(T)a_N$, it follows that $a_N(q - vp^j) = 0$; if $f_a \neq T^*$, then $qa_N = 0$. This is inconsistent with the choice of N , which completes the proof. \square

As a consequence:

Lemma 7. *Suppose that \mathbb{L}/\mathbb{K} is a CM \mathbb{Z}_p -extension in which all the primes above p are totally ramified and \mathbb{K} is chosen such that the conditions in Proposition 2 hold. Then $TA^- \subset D^-$ and there is a decomposition $TA^- = L_t + M_t$ with $L_t \cap M_t \subseteq C^-$; in particular, $T^*L_t \cap T^*M_t = 0$.*

Proof. The primes above p are totally ramified and the base is chosen such that the Proposition 2 holds, thus we can apply complex conjugation, obtaining $TA^- \subset D^-$ and $L_t \cap M_t = C^-$ by definition of the μ and the λ -parts. The final claim follows from $T^*C^- = 0$. Let $w \in T^*L_t^- \cap T^*M_t^-$ be given by $w = T^*x \in T^*L_t^-$, $w = T^*y \in T^*M_t^-$, with $x \in L_t^-$, $y \in M_t^-$. Since obviously $w \in C^-$, we have $T^*w = (T^*)^2y = 0$, so $y \in M_t^- \cap L_t^- = C^-$ and thus $T^*y = 0$. \square

3. THE MAIN THEOREM

We start by fixing the context of fields in which we perform the proof. Suppose that \mathbb{K}_{-3} is a CM number field in which the Leopoldt conjecture is false. As mentioned above, we use negative indices for a sequence of field

extensions which preserve the CM property and have a positive Leopoldt defect, while enjoying an increasing sequence of useful properties. Eventually, $\mathbb{K} = \mathbb{K}_1 \supset \mathbb{K}_{-3}$ will be a ground field for which we are going to prove that $\mathcal{D}(\mathbb{K}) = 0$, thus confirming the claim of Theorem 1. First let $\mathbb{K}_{-2} = \mathbb{K}_{-3}^{(n)}[\zeta_p]$ be the normal closure of \mathbb{K}_{-3} to which we adjoined the p -th roots of unity. Next we choose a small complex abelian extension \mathbf{k} such that $A^-(\mathbf{k}) \neq 1$ and $\mathbf{k} \cap \mathbb{K}_{-2} = \mathbb{Q}$; this extension will be chosen in order to satisfy certain useful properties which are provided in Lemma 8. We let $\mathbb{K}_{-1} = \mathbf{k} \cdot \mathbb{K}_{-2}$. We shall wish to apply the decomposition results above, so we let B be the constant granted by the Theorem of Babaicev and Monsky and p^B also annihilates the \mathbb{Z}_p -torsion of \mathbb{K}_∞ .

Let $n_0 > 0$ be the stabilization index of $L(\mathbb{K}_\infty/\mathbb{K}_{-1})$ and let $n' \geq n_0 + 2B$ be such that for all coherent sequences

$$x = (x_{-1}, x_0, \dots, x_{n'}, \dots) \in A^-(\mathbb{K}_\infty) \setminus (\mathfrak{M}A^-(\mathbb{K}_\infty) + M^-(\mathbb{K}_\infty))$$

we have $\text{ord}(p^B x_{n'}) \geq p^2$.

We define $\mathbb{K} \subset \mathbb{K}_\infty$ such that $[\mathbb{K} : \mathbb{K}_{-1}] = p^{n'+1}$ and $x_{n'} \in A(\mathbb{K})$. From now on \mathbb{K} is our base field. We note that the constant B is not modified by replacing \mathbb{K}_{-1} with \mathbb{K} . The shift of the base field \mathbb{K} induces also a shift of \mathbf{k} which describe in more detail below.

Lemma 8. *There is an imaginary abelian extension \mathbf{k}/\mathbb{Q} and a class sequence $h = (h_n)_{n \in \mathbb{N}} \in A^-(\mathbf{k})$ such that the module $H := \Lambda h$ has rank $p\text{-rk}(H)p(p-1)$ and finite index in $A^-(\mathbf{k})$. Moreover, if $T^k h \in pA^-(\mathbf{k})$, then $k \geq p$ and if D is any integer, \mathbf{k} can be chosen such that the primes dividing D are unramified in \mathbf{k} .*

The proof uses results that will be developed in the next sections and it is provided in §3.3. We let $D = \text{disc}(\mathbb{K}_{-2})$ and use this discriminant in the definition of a field \mathbf{k}' , using Lemma 8; with this, we let $\mathbb{K}_{-1} = \mathbf{k}' \cdot \mathbb{K}_{-2}$, as mentioned above. Then $\mathbb{K}_{-1} \subset \mathbb{K} \subset \mathbb{K}_\infty$ is constructed as in the previous section and we let $\mathbf{k} = \mathbb{K} \cap \mathbf{k}'_\infty$. We also define

$$(17) \quad \Delta = \text{Gal}(\mathbb{K}/\mathbb{Q}), \quad \Delta_0 = \text{Gal}(\mathbf{k}/\mathbb{Q}), \quad \Delta_1 = \text{Gal}(\mathbf{K}/\mathbb{Q}),$$

so $\Delta = \Delta_0 \times \Delta_1$. We then fix a sequence

$$(18) \quad \alpha = (\alpha_n)_{n \in \mathbb{N}} \in A^-(\mathbb{K}_\infty) \quad \text{with} \quad \mathbf{N}_{\mathbb{K}_\infty/\mathbf{k}}(\alpha) = h.$$

The following construction puts in evidence CM \mathbb{Z}_p -extensions whose existence is equivalent to the failure of the Leopoldt conjecture for \mathbb{K} , and in which we shall use the sequence (18).

Lemma 9. *Notations being like above, for arbitrary $n > 0$ there are infinitely many prime ideals $\mathfrak{q} \in \alpha_n$ which are totally split in \mathbb{K}_n/\mathbb{Q} and such that the decomposition group $D(\mathfrak{q}) \subset \text{Gal}(\mathbb{M}^+/\mathbb{K})$ fixes an extension $\mathbb{M}_q^+ \subset \mathbb{M}^+$ with $\mathbb{K}_n \subset \mathbb{M}_q^+$ and $\mathbb{Z}_p\text{-rk}(\text{Gal}(\mathbb{M}_q^+/\mathbb{K}_n)) > 0$.*

In particular, there is a CM \mathbb{Z}_p -extension \mathbb{L}/\mathbb{K} which contains \mathbb{K}_n and in which \mathfrak{q} is totally split.

Proof. Let $\mathfrak{q} \in \alpha_n$ be a prime ideal which is totally split in \mathbb{K}/\mathbb{Q} and coprime to p . By a classical application of Tchebotarew's Theorem, there are infinitely many such primes. Since \mathfrak{q} is coprime with p and all the primes that ramify in \mathbb{M}^+/\mathbb{K} lay above p , it follows that $D(\mathfrak{q}) \cong \mathbb{Z}_p$. Indeed, \mathfrak{q} is totally inert in $\mathbb{K}_\infty/\mathbb{K}_{n'}$ for some $n' > n$, so we have $\mathbb{Z}_p\text{-rk}(D(\mathfrak{q})) \geq 1$; since \mathbb{Q}_q has only one (unramified) \mathbb{Z}_p -extension, it follows that *ess.* $p\text{-rk}(D(\mathfrak{q})) = 1$. But $\text{Gal}(\mathbb{M}^+/\mathbb{K}) \cong \mathbb{Z}_p^{\mathcal{D}(\mathbb{K})+1}$ has no finite subgroups and thus $D(\mathfrak{q}) \cong \mathbb{Z}_p$, as claimed. Moreover, $\mathbb{K}_n \subset \mathbb{M}_q^+ := \mathbb{M}^{+D(\mathfrak{q})}$ since we chose \mathfrak{q} to be completely split in \mathbb{K}_n . We have $\mathbb{Z}_p\text{-rk}(\text{Gal}(\mathbb{M}_q^+/\mathbb{K})) = \mathcal{D}(\mathbb{K}) > 0$ and there is in particular some CM \mathbb{Z}_p -extension $\mathbb{L} \subset \mathbb{M}_q^+$. By definition, $\mathbb{L} \cap \mathbb{K}_\infty \supseteq \mathbb{K}_n$ and the prime \mathfrak{q} is totally split in \mathbb{L} . \square

3.1. Thaine shift and the main coherent sequences. We let \mathbb{K} be a galois CM extension constructed as above, so we assume in addition that stabilization occurs from the first level in the following sense

- A. For all $x \in A^-(\mathbb{K}_\infty) \setminus (\mathfrak{M}A^-(\mathbb{K}_\infty) + M^-(\mathbb{K}_\infty))$ we have $\text{ord}(p^B x_1) > p$ where p^B is an exponent for the μ -part of all the \mathbb{Z}_p -extensions of \mathbb{K} (the existence of which follows from Theorem 2).
- B. The shift equation $px_n = \iota_{n-1,n}(x_{n-1})$ holds for all $n \in \mathbb{N}$ and $x \in L(A^-)$ with $x_{n-1} \neq 0$.
- C. We have $\mu_{p^k} \subset \mathbb{K}$ but $\mu_{p^{k+1}} \not\subset \mathbb{K}$ and $\mathbb{K} = \mathbb{K}_1 = \dots \mathbb{K}_k \subsetneq \mathbb{K}_{k+1}$

Let $N = 2M > 0$ be an integer to be determined below and let \mathbb{L}/\mathbb{K} be some \mathbb{Z}_p -extension with $\mathbb{L} \cap \mathbb{K}_\infty \supseteq \mathbb{K}_N$, for instance the one constructed before; the case $\mathbb{L} = \mathbb{K}_\infty$ is in particular allowed too. We define the following *Thaine shift extensions*: let $\mathfrak{r} \in \alpha_n, n \leq N$ be some totally split prime which is inert in $\mathbb{K}_{n+1}/\mathbb{K}_n$ and $r \equiv 1 \pmod p$ be the rational prime above \mathfrak{r} ; we let $\mathbb{F} \subset \mathbb{Q}[\zeta_r]$ be the subfield of degree p over \mathbb{Q} . Since \mathfrak{r} is totally split in \mathbb{K} while r is ramified in \mathbb{F} , we have $\mathbb{K} \cap \mathbb{F} = \mathbb{Q}$. We let $F = \text{Gal}(\mathbb{F}/\mathbb{Q})$ be generated by $\nu = \nu_r$, let $s = s_r = \nu_r - 1$ and write $\mathcal{N}_a = \mathbf{N}_{\mathbb{F}/\mathbb{Q}}$ for the arithmetic norm, while the algebraic norm is

$$(19) \quad \mathcal{N} = \sum_{i=0}^{p-1} \nu^i = pu(s) + s^{p-1} = p + sf(s),$$

$$f \in \mathbb{Z}_p[X], \quad u \in (\mathbb{Z}_p[s])^\times.$$

We define $\mathbb{K}^{(r)} = \mathbb{K} \cdot \mathbb{F}$ and $\mathbb{L}_n^{(r)} = \mathbb{L}_n \cdot \mathbb{F}$, $\mathbb{L}^{(r)} = \mathbb{L} \cdot \mathbb{F}$. The galois groups $\Delta := \text{Gal}(\mathbb{K}/\mathbb{Q}), \Gamma := \text{Gal}(\mathbb{L}/\mathbb{K})$ commute with F and thus $\text{Gal}(\mathbb{K}^{(r)}/\mathbb{Q}) = F \times \Delta, \text{Gal}(\mathbb{L}^{(r)}/\mathbb{K}^{(r)}) = \Gamma, \text{Gal}(\mathbb{L}^{(r)}/\mathbb{K}) = F \times \Gamma$.

I In the case when $n < N$ and \mathfrak{r} is inert in \mathbb{L} , we say that $\mathbb{L}^{(r)}/\mathbb{L}$ is an *inert Thaine shift*.

S. If $\mathfrak{r} = \mathfrak{q}$ is totally split in \mathbb{L} we speak of a *split Thaine shift*.

The split case is applied for the proof of Theorem 1, while the inert shift is used in the construction of the auxiliary extension \mathbf{k} in Lemma 8. In the

split case, $\mathbb{L} \cap \mathbb{K}_\infty =: \mathbb{K}_N = \mathbb{L}_N$ for some $N = 2M > 0$, where $\mathbb{L} = \mathbb{L}^{(q)}$. The prime $\mathfrak{q} \subset \mathbb{K}_N$ is totally split in \mathbb{L}/\mathbb{Q} and we let $(\mathfrak{q}_m)_{m \in \mathbb{N}}$ with $\mathfrak{q}_m \subset \mathbb{L}_m$ be a norm coherent sequence of primes above \mathfrak{q} . Moreover, we assume that \mathfrak{q} is inert in $\mathbb{K}_{N+1}/\mathbb{K}_N$ and if q is the rational prime below \mathfrak{q} , then $q \equiv 1 \pmod{p^N}$. In the split Thaine shifts of our context, we shall assume that q verifies this conditions. We shall denote by $\xi \in \mu_{p^N}$ a primitive root of unity, so $\xi \in \mathbb{L}'_n$ generates the group of p -roots of unity, for all n . As a consequence, we have

Fact 4. *Let \mathbb{L}'/\mathbb{L} be a Thaine split shift and the related conditions and notations be like above. Then $\xi \notin \mathcal{N}((\mathbb{L}'_n)^\times)$ for all $n > N$. Moreover, if $d = [\mathbb{K}_N^+ : \mathbb{Q}]$, then*

$$(20) \quad |(\mathbb{L}_n^\times)^- / \mathcal{N}((\mathbb{L}'_n^\times)^-)| = p^{p^{n-N}d}.$$

Proof. This is a direct consequence of the Hasse norm principle. Let indeed $\mathfrak{r} \subset \mathbb{L}_n$ be any prime above q , thus any of the primes that ramify in $\mathbb{L}'_n/\mathbb{L}_n$; the claim follows by showing that ξ is not in the local norm image. Since \mathfrak{r} is totally split, the residue field is \mathbb{F}_q and the p -Sylow of the multiplicative subgroup has size $|(\mathbb{F}_q^\times)_p| = p^N$. Local class field theory implies that the norm image has index p , so it is a cyclic subgroup $C_{p^{N-1}}$ and can therefore not contain the full image of the p^N -th roots of unity. A fortiori, $\xi \notin \mathcal{N}((\mathbb{L}'_n)^\times)$ for all $n > N$, which completes the proof of the first statement. Note that the number of pairs of conjugate primes above q in \mathbb{L}_n is $R := p^{p^{n-N}d}$ and the Hasse Norm Principle implies that the size of the norm defect $\mathbb{L}_n^\times / \mathcal{N}(\mathbb{L}'_n^\times)$ is equal to the product of the local norm defects at each of these ramified primes – which are the only primes that ramify in $\mathbb{L}'_n/\mathbb{L}_n$. Since we have seen that the local norm defects are groups of order p , the claim (20) follows by taking minus parts. \square

The primes \mathfrak{q}_m are totally ramified in \mathbb{L}'_m and we let $\mathfrak{Q}_m \subset \mathbb{L}'_m$ be the ramified prime above \mathfrak{q}_m ; in particular \mathfrak{Q}_0 is the prime of \mathbb{K}_N above \mathfrak{q} . This leads to the definition of two sequences which play a crucial role in our proof: we let

$$(21) \quad \begin{aligned} a_m &= [\mathfrak{q}_m^{1-j}], \quad \text{for } m \geq N \text{ and } a_m = \mathbf{N}_{N,m}(a_m), \quad m < N, \\ b_m &= [\mathfrak{Q}_m^{1-j}], \quad \text{for } m \geq N \text{ and } b_m = \mathbf{N}_{N,m}(b_m), \quad m < N, \\ a &= (a_m)_{m \in \mathbb{N}} \in A^-(\mathbb{L}), \quad b = (b_m)_{m \in \mathbb{N}} \in A^-(\mathbb{L}'). \end{aligned}$$

It follows from the definition that $h_n = \mathbf{N}_{K_n, \mathbf{k}_n}(a_n)$ for $n \leq N$ and $b = pa$, as sequences and thus at all levels, due to ramification. We let $C' = F(\mathbb{L}') \subset A^-(\mathbb{L}')$ be the maximal finite submodule. The following lemma indicates the choice of N :

Lemma 10. *Notations being the ones above, one can choose $N = 2M$ such that there are $a_\lambda \in L^-(\mathbb{L}), a_\mu \in M^-(\mathbb{L})$ with $a = a_\lambda + \omega_M a_\mu$ and $\omega_M \cdot M(A^-) \cap F = 0$. Moreover, $Tb \in D^-(\mathbb{L}')$.*

Proof. Let $f \in \mathbb{Z}_p[T]$ be the annihilator polynomial of α defined in (18), so $fa_N = 0$. The base field was chosen such that $Ta \in D^-(\mathbb{L})$, so let $Ta = a'_\lambda + a'_\mu$. Since $fa_N = 0$, an application of Iwasawa's Theorem 6 implies that there is an $x \in A^-(\mathbb{L})$ for which we have

$$fTa_N = \omega_N x = f(T) \cdot (a'_\lambda + a'_\mu) = \nu_{N,1}(x_\lambda + x_\mu).$$

By comparing parts - and using the fact that the intersection $L^- \cap M^- \subset C^-$ is annihilated by T^* , we obtain $f(T)T^*a'_\mu = \nu_{N,1}T^*x_\mu$. Euclidean division yields $\nu_{N,1} = g(T)f + r(T)$, so that for sufficiently large N we have $r(T) \equiv 0 \pmod{p^B}$. For such N , $\nu_{N,1}x_\mu = f(T)g(T)x_\mu$ and thus $f(T)(a'_\mu - g(T)x_\mu) = 0$. Since μ -parts are not annihilated by distinguished polynomials, it follows that $a'_\mu = g(T)x_\mu$. We still have to show that we may choose $N = 2M$ such $g(T) \equiv \omega_M h(T) \pmod{p^B}$, which is equivalent to $\nu_{2M,1} \equiv h(T)f(T)\omega_M \pmod{p^B}$. Once again, Euclidean division yields $\nu_{2M,1} = Q(T) \cdot (f(T)\omega_M) + R_M(T)$. For all roots $\xi \in \overline{\mathbb{Q}_p}$ of $f(T)\omega_M$ we have

$$\nu_{2M,1}(\xi) = \frac{(\xi + 1)^{p^{2M}} - 1}{(\xi + 1)^{p^k} - 1} = R_M(\xi),$$

It suffices thus to take M large enough, so that the global p -adic valuation is $v_p(R_M(\xi)) > B$ for all zeroes of f and ω_M . Since for f , the zeroes are fixed, the problem is solved by taking M sufficiently large. For zeroes of ω_M we use the development $\nu_{2M,1} = \nu_{M,1} \cdot (p^M + O(\omega_M))$. It follows that for sufficiently large $N = 2M$, we have $\nu_{2M,1} \equiv Q_1(T)f(T)\omega_M \pmod{p^B}$ and we may also assume that the quotient Q_1 has free coefficient $Q_1(0) \equiv 0 \pmod{p^B}$, so $Q_1(T) \equiv TQ_2(T) \pmod{p^B}$. Letting $y = Q_2(T)x_\mu$ we have found that $a'_\mu = \omega_M Ty$. Then $T(a - \omega_M y) = a'_\lambda \in L$, so $a - \omega_M y \in L$ too, thus $a = \omega_M y + w, w \in L$, which yields the claimed decomposition.

Finally, since $pb = a$, we may apply Lemma 4 and deduce that $Tb \in D^-(\mathbb{L}')$, after eventually shifting the base field up by one level. Since $F = \text{Ker}(\psi : M(A^-) \rightarrow \mathcal{E}(M))$ for any pseudoisomorphism ψ , we can choose M sufficiently large, such that $\omega_M \psi$ is injective, which implies $\omega_M M(A^-) \cap F = 0$. \square

There are thus $b_\lambda \in L^-(\mathbb{L}'), b_\mu \in M^-(\mathbb{L}')$ with $Tb = b_\lambda + b_\mu$. From $sb = 0$ we also have $sb_\lambda = -sb_\mu \in L^- \cap M^- = C' \cap \text{Ker}(\mathcal{N}) = C'[p] = C[p] \subset A^-(\mathbb{L})$, so $s^2b_\lambda = 0$; also, $psb_\lambda = Tsb_\lambda = 0$. Consequently, $\mathcal{N}(b_\lambda) = pu(s)b_\lambda + s^{p-1}b_\lambda = pb_\lambda$ and $\mathcal{N}(b_\mu) = pb_\mu$. Since $p(b_\lambda + b_\mu) = pTb = Ta = T(a_\lambda + \omega_M a_\mu)$, it follows by comparing parts that $Ta_\lambda - pb_\lambda = pb_\mu - T\omega_M a_\mu = \gamma \in C^-$. Upon multiplication by T^* we obtain $pT^*b_\lambda = TT^*a_\lambda$. The same proof yields $pT^*b_\mu = TT^*a_\mu$.

We have the following defining relations:

$$(22) \quad \begin{aligned} pb &= \mathcal{N}(b) = a, & sb &= 0 \\ Tb &= b_\lambda + b_\mu, & TT^*a_\lambda &= pT^*b_\lambda, & pT^*b_\mu &= \omega_M TT^*a'_\mu. \end{aligned}$$

Since we have shown above that $s(Tb_\lambda) = s(Tb_\mu) = 0$, it will be important to investigate in more detail the group cohomology $H^0(F, A^-(\mathbb{L}'))$. This is done in the next section, in which we also show that $b_\mu \neq 0$.

3.2. Cohomology and the Hasse obstruction module. In this section we investigate the Tate cohomology groups in inert and in split Thaine shifts. Let \mathbb{K} be a fixed galois CM extension containing the p -th roots of unity, and \mathbb{L}/\mathbb{K} be a CM \mathbb{Z}_p -extension with $\mathbb{L} \cap \mathbb{K}_\infty = \mathbb{K}_N$, and we let $\mathbb{L}' = \mathbb{L} \cdot \mathbb{F}$ be a Thaine shift. Thus the extension tower can be the one defined in the previous section, but the above are the only prerequisites that we shall need in this section. The Tate-cohomologies in Thaine shifts are governed by the Hasse Norm Principle and similar properties which are ingredients of the proof of Chevalley's Theorem, also called the ambig class formula [14], Chapter 13, Lemma 4.1. These facts allow comprehensive descriptions of the groups. Here we only focus on the facts that are directly needed in our subsequent proof.

We consider first the case when \mathbb{L}'/\mathbb{L} is a *split Thaine shift*, and let like above $\mathfrak{q}_n \subset \mathbb{L}_n$ build a norm coherent sequence of split primes above $\mathfrak{q} \in a_N$; let $a_n := [\mathfrak{q}_n^{1-j}]$ and $\mathfrak{Q}_n \subset \mathbb{L}'_n$ be the ramified ideals above \mathfrak{q}_n , while $b_n = [\mathfrak{Q}_n^{1-j}]$. Since \mathfrak{q} is assumed to be totally split above \mathbb{Q} , there are $D_N := [\mathbb{K}_N : \mathbb{Q}]/2$ pairs of complex conjugates primes above q in \mathbb{K}_N , with $(q) = \mathbb{Z} \cap \mathfrak{q}$. We assume that r' of these are totally split in \mathbb{L} and let $\tau_i \in \Delta_N := \text{Gal}(\mathbb{K}_N/\mathbb{Q})$ with $\tau_1 = 1$ and $i \leq r'$ be automorphisms such that $\mathcal{R} = \{\mathfrak{q}^{(i)} := \tau_i \mathfrak{q} : i = 1, 2, \dots, r'\}$ be these totally split primes. We denote by $(\mathfrak{q}_n^{(i)})_{n \in \mathbb{N}}$ some fixed norm coherent sequences of primes above $\mathfrak{q}^{(i)}$ and let the class sequences $a^{(i)}, b^{(i)}$ be defined with respect to these sequence, by analogy to the way a, b were defined with respect to \mathfrak{q}_n . We may write, with some abuse of language, $\mathfrak{q}^{(i)} = \tau_i \mathfrak{q}$, $a^{(i)} = \tau_i a$, $b^{(i)} = \tau_i b$. Let $f = f_a(T) \in \mathbb{Z}_p[T]$ be the minimal annihilator polynomial of a and note that f also annihilates $\Lambda b / (\Lambda b \cap M)$.

Therefore $z := f_a(T)T^* \in M^-$ is such that $\Lambda z \cap F = 0$ and thus $\Lambda z \cong \Lambda/p^e$ for some fixed exponent e . If $z^{(i)} = \tau_i z = f_a(T)T^* \tau_i b$, then $\Lambda z^{(i)} \cong \Lambda/p^{e(i)}$ for some $e(i) > 0$. Let $r \leq r'$ and the ordering of the $z^{(i)}$ be such that

$$M_B := \sum_{i=1}^{r'} \Lambda z^{(i)} = \sum_{i=1}^r \Lambda z^{(i)},$$

and r be minimal with this property; i.e. $\{z^{(i)}, i = 1, 2, \dots, r\}$ is a minimal spanning set for the Λ -module M_B . We claim that $M_B = \bigoplus_{i=1}^r \Lambda z^{(i)}$. Indeed, let $\psi : M_B \rightarrow \mathcal{E}(M_B)$ be a pseudoisomorphism. Since the kernel is a finite Λ -module, while $M_B \subset T^*M$ contains no finite submodules, it follows that ψ is injective, so M_B is a direct sum. The claim now follows by induction. We show that every span of m terms in M_B is a direct sum. This is true for $m = 1$. Suppose that the claim holds for all $n < m$ but there is, after eventual reordering, a sum $x = \sum_{i=1}^m c_i(T)z^{(i)} = 0$.

We assume that $v_p(c_m)$ is minimal, so the identity can be rewritten as $p^a(v_m(T)z^{(m)} + y) = 0$, with $v_m \in \mathbb{Z}_p[T]$ a distinguished polynomial and $y \in \sum_{i=1}^{m-1} \Lambda b^{(i)}$. Let $\psi(b^{(i)}) = E_i$ and let $M'_B = \bigoplus_{i=1}^{m-1} \Lambda E_i \subset \psi(M_B)$. We assume that $E_m, \dots, E_r \in \mathcal{E}(M_B) \setminus M'_B$ are chosen in order to complete a Λ -base of $\mathcal{E}(M_B)$. We let $\psi' = \psi|_{\bigoplus_{i=m}^r \Lambda E_i}$ and $w = p^a z^{(m)}$. Then $\psi'(v_m(T)w) = 0$ so injectivity implies that $p^a z^{(m)}$ is a finite torsion element. But $M_B \cap C^- = 0$ so $p^a z^{(m)} = 0$, which confirms that $x = 0$ and completes the proof by induction.

We note that if $(\mathbf{q}'_n)^{(i)}$ is some other sequence above $\mathbf{q}^{(i)}$ and $(b'_n)^{(i)}$ are the respective classes, then $b^{(i)} - b'^{(i)} \in \omega_N A^-(\mathbb{L}')$ and in particular, both sequences have the same image in $H^0(F, A^-(\mathbb{L}'))/(T^{p^N})$. We assume that $r \leq r'$ is maximal such that the classes $\tau_i b$ are Λ -independent. In particular, r does not depend on the choice of $b^{(i)}$.

We have shown:

Lemma 11. *Let $\mathcal{R} = \{\mathbf{q}^{(i)} := \tau_i \mathbf{q} : i = 1, 2, \dots, r'\}$ be the set of all conjugates of \mathbf{q} which are totally split in \mathbb{L} and let $\tau_i b$ be defined as above, while $\tau_i z = f_a(T)T^* \tau_i b$, and $f_a(T)$ is the minimal annihilator of $a_\lambda \in A^-(\mathbb{L})$. Then there is a constant $r \leq r'$ such that*

$$M_B := \sum_{i=1}^r \Lambda \tau_i z = \sum_{i=1}^{r'} \Lambda \tau_i z,$$

and r is minimal with that property and the sum is direct.

With these notations we also have

Lemma 12. *Let \mathbb{L}/\mathbb{K} be a CM \mathbb{Z}_p -extension with $\mathbb{L} \cap \mathbb{K}_\infty = \mathbb{K}_N$ and which allows a split Thaine shift \mathbb{L}'/\mathbb{L} . Let the notations introduced above for primes and their classes hold; then*

$$(23) \quad \text{Ker} (s : A^-(\mathbb{L}') \rightarrow A^-(\mathbb{L}')) = \iota(A^-(\mathbb{L})) + \sum_{j=1}^r \Lambda \tau_j(b).$$

Proof. Let for $n > 0$ the group $T_n \subset A^-(\mathbb{L}'_n)$ be the Λ -module spanned by classes of ramified ideals, thus $T_n \supseteq [b_n^{(i)}; i = 1, 2, \dots, r]_{\mathbb{Z}}$. Since finitely many primes above \mathbf{q} are inert, while the only ramified primes in \mathbb{L}'/\mathbb{L} are the primes above q , it follows that equality holds for sufficiently large n .

Let $n > N$ be arbitrary and $c \in A_n^-(\mathbb{L}'_n)$ have non trivial image $\bar{c} \in H^0(F, A_n^-)$. If $\mathfrak{C} \in c$ then $\mathfrak{C}^s = (\gamma)$ and $(\mathcal{N}(\gamma)) = (1)$. There is thus a unit $\delta \in \mathbb{L}_n$ with $\mathcal{N}(\gamma) = \delta$, as algebraic numbers. Let $\xi \in \mu_{p^N}$ generate the p -roots of unity in \mathbb{L}'_N . The Kronecker unit theorem implies

$$\mathcal{N}\left(\frac{\gamma}{\bar{\gamma}}\right) = \xi^e, \quad e \in \mathbb{Z}.$$

By Fact 4, $\xi \notin \mathcal{N}(\mathbb{L}')$ and therefore $e = pe' \equiv 0 \pmod{p}$. Then $\xi^e \in \mathcal{N}((\mathbb{L}'_n)^\times)$ and by applying Hilbert's Theorem 90, it follows after eventually modifying

γ by some root of unity, that $\gamma^{1-j} = x^s$ for some $x \in \mathbb{L}'_n$. Consequently $(\mathfrak{C}^{1-j}/(x))^s = (1)$ and the class $a^2 = [\mathfrak{C}^{1-j}/(x)]$ contains an ambig ideal; since $a \notin \iota(A^-(\mathbb{L}_n))$, we must even have $a^2 \in T_n$, which implies the claim. \square

As a consequence, we have the following stronger result:

Proposition 4. *Let $\mathbb{L}' = \mathbb{L} \cdot \mathbb{F}$ be a split Thaine shift with $F = \text{Gal}(\mathbb{F}/\mathbb{Q}) = \langle \nu \rangle = \langle s+1 \rangle$ and let $\tau_i \mathfrak{q}, i = 1, 2, \dots, r$ be the conjugates of \mathfrak{q} that are totally split in \mathbb{L}/\mathbb{K} , while $\tau_i b_n, \tau_i b$ are the classes defined previously in this context. Then*

$$H^0(F, A^-(\mathbb{L}')) \cong \bigoplus_{i=1}^r \mathbb{F}_p[[T]] \tau_i \bar{b}$$

is a free $\mathbb{F}_p[[T]]$ module of rank $r > 0$; here the $\tau_i \bar{b}$ are the images of $\tau_i b$ in $H^0(F, A^-(\mathbb{L}'))$. We have $\mu(\mathbb{L}') \geq r$.

Proof. We already know from the previous lemma that $H^0(F, A^-(\mathbb{L}')) \cong M_B/M_B \cap \iota(A^-(\mathbb{L}'))$ with $M_B = \sum_{i=1}^r \Lambda \tau_i(b)$. By ramification, we have $pb = \iota(a)$ and thus $pH^0(F, A^-(\mathbb{L}')) = 0$, which makes H^0 into an $\mathbb{F}_p[[T]]$ module. We have shown in Lemma 11 that M_B is free of $\mathbb{F}_p[[T]]$ -rank r , which implies $\mu(\mathbb{L}') \geq r > 0$.

We are left to prove that $p\text{-rk}(\Lambda b) = \infty$. The relation (20) implies that $|H^1(F, A^-(\mathbb{L}'_n))| \geq p^{p^{n-N}d}$. Indeed, let $R = p^{p^{n-N}d}$ and $\mathfrak{r}, \bar{\mathfrak{r}} \subset \mathbb{L}_n$ one of the R pairs of complex conjugate primes above q . Let $g \in \mathbb{F}_q^\times$ generate the p -Sylow subgroup and let

$$x_{\mathfrak{r}} \in \mathcal{O}(\mathbb{L}_n) \quad \text{with} \quad x_{\mathfrak{r}} \cong \begin{cases} g \bmod \mathfrak{r} & , \\ 1/g \bmod \bar{\mathfrak{r}} & \text{and} , \\ 1 \bmod \mathfrak{r}' \end{cases}$$

for all primes $\mathfrak{r}' \supset q\mathcal{O}(\mathbb{L}_n) \cap (q)$ and $(\mathfrak{r}', \mathfrak{r}\bar{\mathfrak{r}}) = (1)$. By applying the Tchebotarew Theorem to the q -ray class field, we deduce that there is a principal prime ideal (ρ) with $\rho \equiv x_{\mathfrak{r}} \bmod q\mathcal{O}(\mathbb{L}_n)$, which is totally split in \mathbb{L}'_n/\mathbb{Q} . We let $\mathfrak{R} \subset \mathbb{L}'_n$ be the prime above it and $r = [\mathfrak{R}^{1-j}]$; thus r is not p -principal. Otherwise, r is annihilated by some power t with $(t, p) = 1$ and we may assume that $\mathfrak{R}^{t(1-j)} = (\gamma)$. But then $\mathcal{N}(\gamma/\bar{\gamma}) \in \mu_{p^N} \cdot \rho$. Let $P = \prod_{i=1}^{2R} (\mathbb{F}_q^\times)^{(q-1)/p^N} \subset \mathcal{O}(\mathbb{L}_n)/q\mathcal{O}(\mathbb{L}_n)$ be the product of the p groups in the q -ideles of \mathbb{L}_n . The Chinese Remainder Theorem implies that $|P^-(P^-)^p| = R$ and for each residue class in $x \in P^-(P^-)^p$ we may find ρ, \mathfrak{R} as above, such that ρ has image x in $P^-(P^-)^p$ and consequently \mathfrak{R} is not p -principal. This implies our claim. The groups $A^-(\mathbb{L}'_n)$ are finite, so we deduce from the structure of $H^0(F, A^-(\mathbb{L}'_n))$ that

$$p^{s \cdot p\text{-rk}(\Lambda b_n)} = |H^0(F, A^-(\mathbb{L}'_n))| = |H^1(F, A^-(\mathbb{L}'_n))| \geq p^{dp^{n-N}},$$

hence $s \cdot p\text{-rk}(\Lambda b_n) \geq dp^{n-N}$ and thus $p\text{-rk}(\Lambda b_n) \rightarrow \infty$, which implies $b \notin L^-$ and completes the proof. \square

3.3. Completion of the auxiliary constructions. As mentioned previously, the case of inert Thaine shifts will be used in the construction of the auxiliary extension \mathbf{k} . In this case we are particularly interested in the group H^1 , as reflected in

Lemma 13. *Let K be an imaginary quadratic extension of \mathbb{Q} with $A^-(K) = 0$. Let $L = K^{(q)}F$ be an inert Thaine shift, with $\mathfrak{q} \subset K_j$ a totally split, principal prime ideal, that is inert in K_∞/K_j and $F \subset \mathbb{Q}[\zeta_q]$ the cyclic subfield of degree p over \mathbb{Q} . Then $\lambda^-(L) = \varphi(p^j)$ and there is an element $h \in A^-(L) \setminus \mathfrak{M}A^-(L)$ such that $[A^-(L) : \Lambda h] < \infty$. The module $H(p) := \sum_{i=0}^{p^{j-1}-1} \mathbb{Z}_p T^i h$ is a \mathbb{Z}_p -pure submodule of $A^-(L)$: if $p^c x \in H(p)$, then $x \in H(p)$.*

Finally let $U = \omega_l(T)$, $l \geq 1$ and $\Lambda' = \mathbb{Z}_p[[U]]$; considering the \mathbb{Z}_p -extension L_∞/L_l and the induced module $B = A^-(L_\infty/L_l)$ as a Λ' -module, then $H'(p) := \sum_{i=0}^{p^{j-1}-1} \mathbb{Z}_p U^i h \subset B$ is also a \mathbb{Z}_p -pure module.

Proof. We start by choosing $K = \mathbb{Q}[\sqrt{-d}]$, an imaginary quadratic extension with $p \nmid h(K)$ and $\left(\frac{-d}{p}\right) = -1$. Such a field can be found since the analytic class number formula and bounds yield $h(K) < \sqrt{d} < p$ for $d < cp^2$, a range in which a discriminant can be found, which also verifies the quadratic reciprocity condition, requiring that p is inert in K .

Let $\mathfrak{q} \in K_j$ be a principal prime which is totally split over \mathbb{Q} and inert in K_{j+1}/K_j , let q be the rational prime below it. We assume that $q \equiv 1 \pmod{p^j}$, which can be achieved by an application of Tchebotarew: consider the compositum $H[\zeta_p]$ with H/K the maximal abelian unramified extension. Then \mathfrak{q} should be totally split in $H[\zeta_p]$, the existence being granted by Tchebotarew. Let $\mathbb{F} \subset \mathbb{Q}[\zeta_q]$ the subfield of degree p , so $\mathbb{F} \cap K = \mathbb{Q}$ since q is unramified in K but totally ramified in \mathbb{F} . Let $L = \mathbb{K} \cdot \mathbb{F}$. Then, an application of Kida's formula implies that $A^-(L) = (p-1)p^{j-1}$: indeed, there are p^{j-1} pairs of complex conjugate primes that ramify in L_j/K_j and since they are inert in L_∞/L_j , there are as many pairs of ramified primes in L_∞/K_∞ . Since K contains no p -th roots of unity and the ramification index is $e = p$ for all ramified primes while $\mu(L_\infty) = 0$, the Kida formula yields

$$\lambda^-(L) = [L : K]\lambda^-(K) + (e-1) \cdot [K_j : \mathbb{Q}]/2 = 0 + (p-1)p^{j-1},$$

as claimed.

We let $F = \text{Gal}(L/K)$, $\nu' \in F$ be a generator and $t = \nu' - 1$ and estimate $H^1(F, A^-(L_n))$ in a similar way to the one used for the split case above. Let $g \in \mathbb{F}_q^\times$ be a generator of this group and $\gamma = g^{(q-1)/p^j}$. Since \mathfrak{q} is totally

split in K_j we have

$$\begin{aligned}
 (24) \quad \mathcal{O}(K_j)/(q\mathcal{O}(K_j)) &\cong \prod_{i=1}^{p^j-1} (\mathcal{O}(K_j)/\tau^i \mathfrak{q} \mathcal{O}(K_j) \times \mathcal{O}(K_j)/\tau^i \bar{\mathfrak{q}} \mathcal{O}(K_j)) \\
 &\cong \prod_{i=1}^{p^j-1} (\mathbb{F}_q \times \mathbb{F}_q).
 \end{aligned}$$

If $x \in (K_j^\times)^{1-j}$ and $x \equiv h \pmod{\tau^i \mathfrak{q}}$ then complex conjugation induces $x \equiv 1/h \pmod{\tau^i \bar{\mathfrak{q}}}$, for any (fixed) value of i . Let $w \in (K_j^\times)^{1-j}$ be such that

$$w \equiv \begin{cases} \gamma \pmod{\mathfrak{q}} \\ 1/\gamma \pmod{\bar{\mathfrak{q}}} \end{cases} \quad \text{and} \quad \begin{cases} 1 \pmod{\mathfrak{r}} \end{cases} \quad \text{for all other primes } \mathfrak{r} \subset K_j \text{ above } q.$$

Let $\pi : (\mathcal{O}(K_j))_q \rightarrow \mathcal{O}(K_j)/(q)$ be the natural projection of the algebraic semilocalization at the primes above q and $R = \mathbb{Z}_p[T]\pi(w)$; we note that R is the p -Sylow subgroup of the minus part of the multiplicative group in (24). All the primes above q are ramified in L/K and these are the only ramified primes. Since K_j contains no p -th roots of unity, the Hasse Norm Principle implies that

$$N_D := \left(K_j^\times / \mathcal{N}(L_j^\times) \right)^{1-j} \cong R/R^p.$$

We claim that there is a group isomorphism $\psi : H^1(F, A^-(L_j)) \rightarrow R/R^p$. For this we note first that for $x \in A^-(L_j)$ we necessarily have $\mathcal{N}(x) = 0$, by choice of K . Thus $H^1(F, A^-(L_j)) = A^-(L_j)/(tA^-(L_j))$, while $\mathcal{N} = pu(t) + t^{p-1}$ readily implies that p annihilates $H^1(F, A^-(L_j))$. Let now $x \in A^-(L_j)$ with non trivial image $\bar{x} \in H^1(F, A^-(L_j))$ and let $\mathfrak{R} \in x$ be a totally split prime. Then $(\rho) = \mathcal{N}(\mathfrak{R})$ (must be a principal prime and we claim that $\pi(\rho^{1-j}) \notin R^p$. Otherwise, $\rho^{1-j} \in \mathcal{N}(L_j^\times)$ and we may assume that $\rho^{1-j} = \mathcal{N}(y^{1-j})$, so in terms of ideals $\mathcal{N}(\mathfrak{R}/(y))^{1-j} = (1)$ and thus $(\mathfrak{R}/(y))^{1-j} = \mathfrak{D}^s$, for some ideal $\mathfrak{D} \subset L_j$. This implies that $x \in \mathbb{A}^-(L_j)^s$ and thus $\bar{x} = 1$, which contradicts the choice of \mathfrak{R} . We define $\psi(x) = \pi'(\rho)$ where $\pi' : (\mathcal{O}(K_j))_q \rightarrow R/R^p$ is the composition of π with the natural map $R \rightarrow R/R^p$. A direct verification establishes that ψ is a well defined map of $\mathbb{F}_p[T]$ -modules; we leave these details to the reader and show that ψ is a bijection. We have shown that $\psi(x) = 1$ iff $x = 1$, so ψ is injective; it is also surjective. For this we consider some principal prime $(\rho) \subset K_j$ which is totally split in L_j/\mathbb{Q} , with $r := \pi'(\rho/\bar{\rho}) \in R/R^p$ and $r \neq 1$. Such a prime can be determined with Tchebotarew's Theorem, by considering the q -ray class field $H_q \supset K_j$, which also contains L_j . If \mathfrak{R} is the split prime above (ρ) , then $\mathfrak{R}/\bar{\mathfrak{R}}$ cannot be principal, since otherwise $\rho/\bar{\rho} \in \mathcal{N}(L_j^\times)$ in contradiction with $r \neq 1$. Letting $x = [\mathfrak{R}] \in A^-(L_j)$ we see by construction that $\psi(x) = r$ and thus ψ is surjective.

Since the module R/R^p is a $\mathbb{F}_p[T]$ -cyclic of order p^{j-1} , it follows that $H^1(F, A^-(L_j))$ is $\mathbb{F}_p[T]$ cyclic of order p^{j-1} too. We let $h = \psi^{-1}(\pi'(w))$, where $\psi'(w)$ generates R/R^p as an $\mathbb{F}_p[T]$ module. We note that R, w, h, ψ all depend on j and, for all $n \geq j$ there is a module R_n and a bijection of $\mathbb{F}_p[T]$ -modules $\psi_n : H^1(F, A^-(L_n)) \rightarrow R_n/R_n^p$, which is constructed in a similar way as above. One may choose a norm coherent sequence $h = (h_n)_{n \in \mathbb{N}}$ such that h_n generates $H^1(F, A^-(L_n))$ as an $\mathbb{F}_p[T]$ -module.

We claim that $[A^-(L) : \Lambda h] < \infty$. Since $\mathcal{N}h = 0$ it follows that $-ph = t^{p-1}u^{-1}(t)h$ so the t -rank of $\Lambda[t]h$ is at most $p-1$; here the t -rank is the rank of $\Lambda[t]h/\Lambda h$. Let $f \in \Lambda$ be the minimal annihilator polynomial of h and $g \in \Lambda$ be the one of $s^k h$ for some $k < p-1$. We claim that $f = g$; we have indeed $f(s^k h) = s^k(fh) = 0$ so $g \mid f$. On the other hand, $s^k gh = 0$ implies that

$$-pgh = (u^{-1}s^{p-1-k})(s^k gh) = 0, \quad \text{hence } gh = 0,$$

so $g \mid f$ too, and thus $f = g$ as claimed.

Assuming now that $[A^-(L) : \Lambda h] = \infty$, it follows that there is some $k < p-1$ such that $\mathbb{Z}_p t^k h \cap \Lambda h = 0$. Suppose there are $c \geq 0, g(T) \in \Lambda$ with $p^c t h = g(T)h$, and by iteration, $p^{(p-1)c} t^{p-1} h = g(T)^{p-1} h = p u(t)h$, so $\mathbb{Z}_p t^k h \cap \Lambda h \neq 0$ for all $k > 0$ and thus $[A^-(L) : \Lambda h] < \infty$. It remains that $\mathbb{Z}_p t h \cap \Lambda h = 0$ and thus $A^-(L) = \bigoplus_{i=0}^{p-2} t^i \Lambda h$, so in particular $\Lambda h \cap t A^-(L) = 0$. However, from $\mathcal{N}h = 0$ we deduce that $ph = -t^{p-1}u^{-1}(t) \in \Lambda h \cap t A^-(L)$. This is a contradiction which implies that this case cannot occur and thus $[A^-(L) : \Lambda h] < \infty$.

Let $G(T) \in \mathbb{Z}_p[T]$ be a distinguished polynomial with $G(T)h = tv(T)h \in t\Lambda h$. We show that $\deg(h) \geq p^{j-1}$; indeed, an iteration yields $G(T)^i h = (v(T)t)^i h$, $0 \leq i < p$. Inserting this relation in $\mathcal{N}h = 0$ we obtain $(G(T)^{p-1} + O(p))h = 0$, so Weierstrass preparation implies that h has an annihilator $H(T) = G(T)^{p-1} + O(p)$ of degree $\deg(H) = (p-1)\deg(G) \geq (p-1)p^{j-1}$. Therefore $\deg(G) \geq p^{j-1}$, as claimed. The same argument implies that $p\text{-rk}(\Lambda h/t\Lambda h) = p^{j-1}$. We have $A^-(L) = \sum_{i=0}^{p-2} t^i \Lambda h$, so for arbitrary $z \in A^-(L)$ there are polynomials $z_i(T) \in \mathbb{Z}_p[T]$ with $\deg(z_i) < p^{j-1}$ such that $z = \sum_{i=0}^{p-2} z_i(T)t^i h$.

We show that the module $H(p) = \sum_{i=0}^{p^{j-1}-1} \mathbb{Z}_p T^i h \subset A^-(L)$ is \mathbb{Z}_p -pure. Indeed, consider $x \in A^-(L)$ such that $p^c x \in H(p)$ for some $c > 0$ and let

$$p^c x = g(T)h = p^c \sum_{i=0}^{p-2} t^i x_i(T)h,$$

with $\deg(g), \deg(x_i) < p^j$. By separating terms, we obtain $(g(T) - p^c x_0(T))h \in t\Lambda h$. Since $\deg(g(T) - p^c x_0(T)) < p^{j-1}$ it follows from the previous remarks, that $g(T) = p^c x_0(T)$, so $p^c x \in p^c \Lambda h$, thus $x \in \Lambda h$, as claimed.

Finally, we prove that the shifted module $H'(p)$ is also pure. First note that $[B : \Lambda' h] < \infty$, the proof being identical with the one above, after

replacing T by U and Λ by Λ' . We obtain a decomposition

$$B = \sum_{i=0}^{p-2} t^i \Lambda' h,$$

and the proof that $H'(p) := \sum_{i=0}^{p^{j-1}-1} \mathbb{Z}_p U^i h$ is \mathbb{Z}_p -pure follows the same pattern as the one for $H(p)$. \square

We now relate the construction above to some given CM field. Let \mathbb{B}/\mathbb{Q} be the \mathbb{Z}_p -extension of \mathbb{Q} and let the intermediate fields be numbered by $\mathbb{B}_1 = \mathbb{Q}$ and $[\mathbb{B}_{n+1} : \mathbb{B}_n] = p$. For a number field \mathbb{M} we let $l = l(\mathbb{M}) \geq 1$ be defined by $\mathbb{M} \cap \mathbb{B} = \mathbb{B}_l$. With this we note the following

Fact 5. *Let \mathbb{M} be a galois CM number field containing the p -th roots of unity with $l = l(\mathbb{M})$ and $d = \text{disc}(\mathbb{M})$. The fields K, L in the Lemma 13 can be chosen such that the fields L, \mathbb{M} are linearly disjoint and $(\text{disc}(L), pd) = 1$.*

Proof. If $K = \mathbb{Q}[\sqrt{D}]$, then $\text{rad}(\text{disc}(L)) = \text{rad}(Dq)$; it suffices thus to choose D and q such that $(\text{rad}(D)q, pd) = 1$. Since the discriminants are coprime, it also follows that L and \mathbb{M} are linearly disjoint, we set $\mathbb{M}' = L \cdot \mathbb{M}$. \square

We can complete the construction of the auxiliary fields in our proof. Let $\mathbb{K}_{-3}, \mathbb{K}_{-2}$ be defined like at the beginning of this chapter. With $d = \text{disc}(\mathbb{K}_{-2})$ we construct K, L as in Lemma 13 and in Fact 5, where we choose $j = 2$, so $p\text{-rk}(A^-(L)) = p(p-1)$. We let \mathbb{K}_{-1} be the smallest field in the cyclotomic \mathbb{Z}_p -extension of the compositum $\mathbb{K}_{-2} \cdot L$, in which conditions A., B. and C. at the beginning of §3.1 hold. Then $\mathbf{k} := L_\infty \cap \mathbb{K}_{-1}$ and $k = l(\mathbb{K}_{-1}) = l(\mathbf{k})$. We choose $N = 2M$ like in Lemma 10 and let $\mathfrak{q} \subset \mathbb{K}_N$ be a totally split prime, such that $\mathfrak{q} \cap \mathbf{k}_N \in h_N$ and \mathbb{L}/\mathbb{K} is a \mathbb{Z}_p -extension with $\mathbb{K}_N = \mathbb{L} \cap \mathbb{K}_\infty$ and \mathfrak{q} totally split in \mathbb{L}/\mathbb{Q} and inert in $\mathbb{K}_\infty/\mathbb{K}_N$. The field $\mathbb{F} \subset \mathbb{Q}[\zeta_q]$ is herewith well defined, and we let $\mathbb{K}' = \mathbb{K} \cdot \mathbb{F}, \mathbb{L}' = \mathbb{L} \cdot \mathbb{F}, \mathbf{k}' = \mathbf{k} \cdot \mathbb{F}$; we let $h' \in A^-(L')$ be a sequence with $N_{L'/L}(h') = h$ and such that $\mathfrak{Q} \cap \mathbf{k}'_N \in h'_N$. Note that $h' \notin \mathfrak{M}A^-(\mathbf{k}'_\infty)$.

If the sequences a, b are defined on base of \mathfrak{q} , as described after Lemma 10, then $b \notin \mathfrak{M}A^-(\mathbb{L}')$. Indeed, $N_{\mathbb{L}', \mathbf{k}'}(b) = h'_N$ and the claim follows from the respective claim on h'_N ; a fortiori, $a \notin \mathfrak{M}A^-(\mathbb{L})$ and $a_N \notin A^-(\mathbb{K}_N)$. As a consequence we have:

Corollary 2. *In the construction defined above, assume that there exists a $\gamma_M \in A^-(\mathbb{K}_M), \gamma_M \neq 0$, and a distinguished polynomial $g(T) \in \mathbb{Z}_p[T]$ such that $p\gamma_M = g(T)a_M \notin \text{Ker}(N : A^-(\mathbb{K}_M) \rightarrow A^-(\mathbf{k}_M))$. Then either $\gamma_M \in \Lambda a_M$ or $\deg(g(T)) > p-1$.*

Proof. Let $w_M = \mathbf{N}_{\mathbb{K}_M/\mathbf{k}_M}(\gamma_M) \in A^-(L_M)$ (we use here the notation $L_M = \mathbf{k}_M$ in conformity with the notation used in the general treatment above). We have shown in Lemma 13 that $H'(p) := \sum_{i=0}^{p-1} \mathbb{Z}_p T^i h$ is a \mathbb{Z}_p -pure module. Due to the choice of \mathbb{K} , we shall have $l(\mathbb{K}) = l(L) \geq 2$ in this case, hence the

notation $H'(p)$ – however, we use the variables $\tau; T = \tau - 1$ for a generator of the galois group in the shifted extension L_∞/L .

We chose $M \gg l(\mathbb{K})$ so in particular, the rank of $A^-(L_n)$ is stable for $n > 1$ and for $x \in A^-(L) \setminus \mathfrak{M}A^-(L)$ we have $x_1 \neq 1$ and $\text{ord}(x_M) \geq p^M$. Let $w \in A^-(L)$ be an arbitrary sequence which coincides with w_M in L_M . Such a sequence is unique modulo $\omega_M A^-(L)$. We have shown that there is a decomposition $w = \sum_{i=0}^{p-2} W_i(T) t^i h$. Taking norms in the identity $p\gamma_M = g(T)a_M$ we obtain

$$pw_M = \sum_{i=0}^{p-2} pW_i(T) t^i h_M = g(T)h_M \quad \Rightarrow \quad (g(T) - pW_0(T))h_M \in t\Lambda h_M.$$

Let $V(t, T) := \sum_{i=0}^{p-3} pW_{i-1}(T) t^i$ and define

$$z := (g(T) - pW_0(T))h, \quad y := tV(t, T)h \in A^-(L).$$

We have $z_M = y_M$, so by Lemma 2 and the choice of L it follows that there is some $Z \in A^-(L)$ with $z = y + \omega_M Z$. Let $Z = \sum Z_i(T) t^i h$, so $(g(T) - pW_0(T) - \omega_M(T))h \in t\Lambda h$. By choice of M we have $\deg(\omega_M) > p^2$, say. If $g(T)$ is not p -divisible, the Weierstrass preparation theorem implies that there is a polynomial $\tilde{g} \in \mathbb{Z}_p[T]$ of degree $\deg(\tilde{g}) = \deg(g)$ and a unit $u(T) \in \Lambda^\times$ such that $u \cdot \tilde{g}h \in t\Lambda h$. Therefore $\tilde{g}h \in tu^{-1}\Lambda h = t\Lambda h$ and the fact that $H'(p)$ is \mathbb{Z}_p -pure implies that $\deg(g) \geq p$. Otherwise, $g(T) = pg_1(T)$ and thus $p(w_M - g_1(T)h_M) = 0$. In this case, we find like previously that $w = g_1(T)h + O(\omega_M)$ and thus $w \in \Lambda h$, which completes the proof. \square

3.4. Proof of the main Theorem. We assume that \mathbb{K}_{-3} is a CM field in which the Leopoldt conjecture fails, and use the auxiliary constructions completed in the previous section, in order to obtain $\mathbb{K}, \mathbb{L}, \mathbb{L}'; a, b, \mathfrak{q}$, etc. Recall that, as noted above (22),

$$sb_\lambda = -sb_\mu \in \text{Ker}(\mathcal{N}) \cap (L^- \cap M^-) = \text{Ker}(\mathcal{N}) \cap C^- = C^-[p].$$

Therefore $Tb_\lambda, Tb_\mu \in \text{Ker}(s)$. The Theorem 1 is proved as follows:

Proof. We show first that $b_\lambda \in \iota(A^-(\mathbb{L}))$. By Proposition 4, $\mathcal{H} := H^0(F, A^-(\mathbb{L}'))$ is a free $\mathbb{F}_p[[T]]$ module of rank $r \geq 1$ and we write $\bar{\cdot} : A^-(\mathbb{L}') \rightarrow \mathcal{H}$ for the natural projection. Since $Tb_\lambda \in \text{Ker}(s)$ and $T^{\deg(f)+1}b_\lambda \in p\Lambda b_\lambda \subset \iota(A^-(\mathbb{L}))$, it follows that $T^{\deg(f)+1}\bar{b}_\lambda = 0$. Thus $\bar{b}_\lambda \in \mathcal{H}$ is a torsion element, and since the module \mathcal{H} is torsion-free, it follows that $\bar{b}_\lambda = 0$ and thus $b_\lambda \in \iota(A^-(\mathbb{L}))$, as claimed. We have $b_\lambda = \iota(\gamma')$ for some $\gamma' \in A^-(\mathbb{L})$ and

$$Ta = Ta_\lambda + T\omega_M a_\mu = \mathcal{N}(Tb) = \mathcal{N}(b_\lambda + b_\mu) = p\gamma' + (T\omega_M a_\mu + pc),$$

for some $c \in C^-(\mathbb{L}')$. Hence, after canceling terms, we obtain

$$Ta_\lambda = p(\gamma' + c), \quad \text{and} \quad p\gamma = TT^*a_\lambda \in \Lambda a_\lambda, \quad \text{for } \gamma := T^*\gamma'.$$

We raise a contradiction by showing that this identity is inconsistent at finite levels. Since $p\gamma = TT^*a_\lambda$ as coherent sequences, the identity holds a fortiori at level M . Letting $g(T) = TT^*$, we notice from the definition

that $a_M = a_{\lambda, M}$ and $TT^*h_M = N_{\mathbb{K}_M/\mathbf{k}_M}(TT^*a_M) \neq 0$. The resulting identity $p\gamma_M = g(T)a_{\lambda, M} = g(T)a_M$ satisfies premises of Corollary 2. Since $\deg(g) = 2 < p$, it follows that $\gamma_M \in \Lambda a_M$, and taking norms, $N(\gamma_M) \in \Lambda h_M$ – where we write $N = N_{\mathbb{K}/\mathbf{k}}$. Let now $\beta_M = N(b_M) \in A^-(L'_M)$ and $y_M = g_2(T)h_M = N(\gamma_M) \in A^-(L_M)$, $z_M = N(b_{\mu, M})$. By definition, we have $pz_M = 0, p\beta_M = h_M$ and consequently

$$Tp\beta_M = Th_M = p(g(T)h_M + z_M) = pTT^*h_M \Rightarrow T(1 - pT^*)h_M = 0.$$

The last identity implies $Th_M = 0$ and thus $p\text{-rk}(\Lambda h_M) = 1$. This contradicts the fact that M was chosen such that $p\text{-rk}(\Lambda h_M) = \lambda^-(L) = p(p-1) > 1$, showing that the extensions, \mathbb{L}, \mathbb{L}' cannot exist and confirms the claim of Theorem 1. \square

4. APPENDIX : PROOF OF PROPOSITION 3

Let $N = A^-(T^*)$ be defined in the cyclotomic \mathbb{Z}_p -extension of \mathbb{K} , and suppose that \mathbb{K} is a CM-extension with positive Leopoldt defect and containing the p -th roots of unity. We have mentioned that $\mathbb{Z}_p\text{-rk}(\text{Gal}(\mathbb{M}^+/\mathbb{K}_\infty)) = \mathcal{D}(\mathbb{K})$, a fact which is proved in all text-books.

Let $\mathbb{M} \subset \Omega(\mathbb{K})$ be the product of all \mathbb{Z}_p -extensions of \mathbb{K} and let $\Phi = \mathbb{M}^- \cap (\mathbb{H}^- \cap \Omega_E)$. One can build an explicit map $\rho : E(\mathbb{K}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \rightarrow \overline{E}$ such that $\text{Ker}(\rho) \sim \text{Rad}(\Phi/\mathbb{K}_\infty)$ and thus $\mathbb{Z}_p\text{-rk}(\text{Gal}(\Phi/\mathbb{K}_\infty)) = \mathcal{D}(\mathbb{K})$ while reflection yields $T^*\text{Gal}(\Phi/\mathbb{K}_\infty) = 0$. The extension Φ was for instance investigated by Jaulent in [9]; we denote it *the phantom field* associated to the Leopoldt conjecture.

The p -ramified, p -abelian, real extensions of \mathbb{K}_∞ are obtained as Kummer extensions by taking roots of classes in A^- , according to the point 2. in Remark 1. In fact, if $\Omega^+ = \Omega^{X^-}$ is the fixed field of the minus part of $X := \text{Gal}(\Omega/\mathbb{K}_\infty)$, we have $\Omega^+ = \overline{\mathbb{K}}_\infty[(A^-)^{1/p^\infty}]$. Here $\overline{\mathbb{K}}$ indicates that we might have to adjoin first the roots of some expressions of the type $\wp/\overline{\wp}$, with \wp a principal prime of \mathbb{K}_∞ above p .

The galois properties of the Kummer pairing imply more precisely that $\mathbb{M}^+ \subset \mathbb{K}_\infty[N^{1/p^\infty}]$, and since $T\text{Gal}(\mathbb{M}^+/\mathbb{K}_\infty) = 0$, it follows that $T^*\text{Rad}(\mathbb{M}^+/\mathbb{K}_\infty) = 0$. Considering $Y := \text{Gal}(\mathbb{K}_\infty[N^{1/p^\infty}]/\mathbb{K}_\infty) \cong N^\bullet$, it follows in fact that $\mathbb{M}^+ = (\mathbb{K}_\infty[N^{1/p^\infty}])^{TY}$. By duality it follows that $\text{Rad}(\mathbb{M}^+/\mathbb{K}_\infty) \cong N/(T^*N)$. There is an exact sequence of pseudoisomorphisms:

$$1 \rightarrow N[T^*] \rightarrow N \rightarrow N \rightarrow N/(T^*N) \rightarrow 1,$$

in which the central map is $T^* : N \rightarrow N$. From this, we deduce

$$\begin{aligned} \mathcal{D}(\mathbb{K}) &= \mathbb{Z}_p\text{-rk}(\text{Gal}(\mathbb{M}^+/\mathbb{K}_\infty)) = \mathbb{Z}_p\text{-rk}(\text{Rad}(\mathbb{M}^+/\mathbb{K}_\infty)) \\ &= \text{ess. } p\text{-rk}(N/T^*N) = \text{ess. } p\text{-rk}(N[T^*]). \end{aligned}$$

We have thus shown that $\text{ess. } p\text{-rk}(A^-[T^*]) = \mathcal{D}(\mathbb{K})$ and for each $\mathbb{L} \subset \mathbb{M}^+$ there is a sequence $a \in A^-(T^*) \setminus T^*A^-(T^*)$ with $\mathbb{L} = \mathbb{K}_\infty[a^{1/p^\infty}]$. This completes the proof of the Proposition 3.

The following useful fact was proved by Sands in [15]:

Lemma 14. *Let \mathbb{L}/\mathbb{K} be a \mathbb{Z}_p -extension of number fields in which all the primes above p are completely ramified. If $F(T) \in \mathbb{Z}_p[T]$ is the minimal annihilator polynomial of $L(\mathbb{L})$, then $(F, \nu_{n,1}) = 1$ for all $n > 1$.*

Acknowledgement 1. *This is an alternative approach to several previous attempts which used λ -type rather than μ -type sequences; with that approach it was only possible to prove the case of the Leopoldt conjecture, in which p is totally split in \mathbb{K} . The new approach grew from discussions with Sören Kleine, related to his PhD thesis that concerns Greenberg's Null Space Conjecture. It is to an important extent due to the involvement of Kleine with μ -extension and the discussions had with him on related subjects, that made the elaboration of this proof possible.*

I thank Cornelius Greither for his careful reading of preliminary drafts of this version. His remarks and the questions he asked during a period of almost one year, helped to substantially improve the quality of the paper and eliminate several flaws. His valuable remarks lead to improvements of the text; in particular the proof of the first two conditions in Lemma 7 is due to him.

I would like to express my gratitude to the precious few who assisted earlier attempts with discussions and comments: Grzegorz Banaszak, John Coates, Ralf Greenberg, Hendrik Lenstra, Florian Pop. Ina Kersten and the colleagues at the Mathematical Institute of Göttingen have provided during many years of evolution, an atmosphere of understanding and encouragement, which was supportive for long time research: to them my sincere gratefulness.

Last but not least, this is to Theres and Seraina, who indulged over years with an ambig family presence of the researcher.

REFERENCES

- [1] J. Ax. On the units of an algebraic number field. *Illinois Journal of Mathematics*, 9:584–589, 1965.
- [2] V. Babaicev. On the linear nature of the behavior of Iwasawa's μ -invariant. *Izv. Akad. Nauk SSSR - Math. USSR Izvetija*, 19(1):1–12, 1982.
- [3] A. Baker. Linear forms in the logarithms of algebraic numbers I, II, III. *Mathematika*, 13, 14:204–216; 102–107, 220–228, 1966, 67.
- [4] A. Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.
- [5] M. Emsalem, H. Kisilevsky, and D. Wales. Indépendance linéaire sur $\overline{\mathbb{Q}}$ de logarithmes p -adiques de nombres algébriques et rang p -adique du groupe des unités d'un corps de nombres. *Journal of Number Theory*, 19:384–391, 1984.
- [6] T. Fukuda. Remarks on \mathbb{Z}_p -extensions of number fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 70(8):264–266, 1994.
- [7] R. Greenberg. On the Iwasawa invariants of totally real fields. *American Journal of Mathematics*, 98:263–284, 1976.
- [8] K. Iwasawa. On \mathbb{Z}_ℓ -extensions of number fields. *Ann. Math. Second Series*, 98:247–326, 1973.
- [9] J. Jaulent. Sur les conjectures de Leopoldt et Gross. In *Journées Arithmétiques de Besançon (1985)*, volume 147–48 of *Astérisque*, pages 107–120, 1987.

- [10] J. Jaulent. Note sur la conjecture de Leopoldt. <http://front.math.ucdavis.edu/0712.2995>, 2007.
- [11] M. Laurent. Rang p - adique d'unités et action de groupes. *J. reine angew. Math.*, 399:81–108, 1989.
- [12] H. Leopoldt. Zur Arithmetik in Abelschen Zahlkörper. *J. Reine Angew. Math*, 209:54–71, 1962.
- [13] P. Monsky. Some Invariants of \mathbb{Z}_p^d -Extensions. *Mathematische Annalen*, 255:229–233, 1981.
- [14] S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer, combined Second Edition edition, 1990.
- [15] J. Sands. On small Iwasawa invariants and imaginary quadratic fields. *Proceedings of the American Mathematical Society*, 112(3):671–684, 1991.
- [16] M. Waldschmidt. Transcendence et exponentielles en plusieurs variables. *Inventiones Mathematicae*, 63, 1981.
- [17] L. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, 1996.

(P. Mihăilescu) MATHEMATISCHES INSTITUT DER UNIVERSITÄT GÖTTINGEN
E-mail address, P. Mihăilescu: `preda@uni-math.gwdg.de`

C'est pour toi que je joue, Alf c'est pour toi,
 Tous les autres m'écoutent, mais toi tu m'entends ...
 Exilé d'Amsterdam vivant en Australie,
 Ulysse qui jamais ne revient sur ses pas ...
 Je suis de ton pays, métèque comme toi,
 Quand il faudra mourir, on se retrouvera¹

To the memory of Alf van der Poorten

ON THE VANISHING OF IWASAWA'S CONSTANT μ FOR THE CYCLOTOMIC \mathbb{Z}_p -EXTENSIONS OF CM NUMBER FIELDS.

PREDA MIHĂILESCU

ABSTRACT. We prove that $\mu = 0$ for the cyclotomic \mathbb{Z}_p -extensions of CM number fields.

CONTENTS

1. Introduction	1
1.1. Plan of the paper and notations	2
1.2. Thaine shift and the main coherent sequences	3
1.3. Auxiliary facts	4
2. On the vanishing of μ	6
References	10

1. INTRODUCTION

Iwasawa gave in his seminal paper [3] from 1973 examples of \mathbb{Z}_p -extensions in which the structural constant $\mu \neq 0$. In the same paper, he proved that if $\mu = 0$ for the cyclotomic \mathbb{Z}_p -extension of some number field \mathbb{K} , then the constant vanishes for any cyclic p -extension of \mathbb{K} – and thus for any number field in the pro- p solvable extension of \mathbb{K} . Iwasawa also suggested in that paper that μ should vanish for the cyclotomic \mathbb{Z}_p -extension of all number fields, a fact which is sometimes called *Iwasawa's conjecture*. The conjecture has been proved by Ferrero and Washington [2] for the case of abelian fields. In this paper, we give an independent proof, which holds for all CM fields:

¹Free after Georges Moustaki, “Grand-père”

Date: Version 1.0 March 31, 2014.

Key words and phrases. 11R23 Iwasawa Theory, 11R27 Units.

Theorem 1. *Let \mathbb{K} be a CM number field. Then Iwasawa's constant μ vanishes for the cyclotomic \mathbb{Z}_p -extension $\mathbb{K}_\infty/\mathbb{K}$.*

1.1. Plan of the paper and notations. This paper is related to the paper [4] on the Leopoldt conjecture for CM extensions and it maintains the notations and terminology introduced there: we will not redefine any basic object which has already been defined there.

The proof uses techniques based on inert Thaine shifts, and several results which have been proved in [4]. Based upon these results concerning decomposition of Λ -modules and their growth, and using two new lemmas, we derive a contradiction from the study of the μ -module induced in an inert Thaine shift by some element of μ -type, assumed to exist in a CM extension of \mathbb{Q} .

If \mathbb{K} is any number field, we write $\mu^{(c)}$ for Iwasawa's μ -constant for the cyclotomic \mathbb{Z}_p -extension. We show

Fact 1. *Let K be a number field for which $\mu^{(c)}(K) \neq 0$ and L/K be a finite extension, which is galois over K . Then $\mu^{(c)}(L) \neq 0$.*

Proof. We reduce the proof to the case of a cyclic Kummer extension of degree p . If $M \subset L$ has degree coprime to p , then $\text{Ker}(\iota : A(K) \rightarrow A(M)) = 0$. Let $M = L^{\text{Gal}(L/K)_p}$ be the fixed field of some p -Sylow subgroup of $\text{Gal}(L/K)$. Then $([M : K], p) = 0$ and thus $\mu^{(c)}(M) \neq 0$. We may assume without loss of generality, that M contains the p -th roots of unity. Since p -Sylow groups are solvable, the extension L/M arises as a sequence of cyclic Kummer extensions of degree p . It will thus suffice to show that if k is a number field with $\mu^{(c)} \neq 0$ and containing the p -th roots of unity and $k' = k[a^{1/p}]$ is a cyclic Kummer extension of degree p , then $\mu^{(c)}(k') \neq 0$. Let $k_n \subset k_\infty$ and $k'_n \subset k'_\infty$ be the intermediate fields of the cyclotomic \mathbb{Z}_p -extensions, let ν generate $\text{Gal}(k'/k)$. Let F/k_∞ be an abelian unramified extension with $\text{Gal}(F/k_\infty) \cong \mathbb{F}_p[[T]]$; such an extension must exist, as a consequence of $\mu^{(c)} > 0$. There is a $\delta \in k_\infty^\times$ such that $F = k_\infty[\delta^{\mathbb{F}_p[[T]]/p}]$. At finite levels, $F_n = k_n[\delta_n^{\mathbb{F}_p[[T]]/p}]$ and we define $F'_n = F_n[a^{1/p}]$ and let $\overline{F}'_n \subset F'_n$ be the maximal subextension which is unramified over k'_n . We have $\overline{F}'_n \supseteq F_n$ and thus $p\text{-rk}(\text{Gal}(\overline{F}'_n/k'_n)) \geq p\text{-rk}(\text{Gal}(F_n/k_n)) \rightarrow \infty$. Consequently, k'_∞ has an unramified elementary p -abelian extension of infinite rank, and the Artin isomorphism implies that $\mu(k') > 0$, which completes the proof. \square

We shall prove the Theorem 1 by contraposition, starting with the assumption that there exists a CM extension K with $\mu^{(c)}(K) \neq 0$. Based on Fact 1, and using results from [4], we may assume that

1. There is a galois CM extension \mathbb{K}/\mathbb{Q} which contains the p -th roots of unity and such that $\mu^{(c)}(\mathbb{K}) > 0$.
2. We have $TA^-(\mathbb{K}) \subset D^-(\mathbb{K})$, where $D(\mathbb{K})$ is the module of decomposed classes.

3. For all $x \in A(\mathbb{K}) \setminus \mathfrak{MA}(\mathbb{K})$ we have $\text{ord}(x_1) \geq p^2$ and if $x \in L^-(\mathbb{K})$ then $\iota_{n,n+1}(x_n) = px_{n+1}$ for all $n > 0$ while $p\text{-rk}(\Lambda x_n)$ is constant.

The first condition is obviously achieved by taking the normal closure of K and adjoining the p -th roots of unity. The second and the third conditions are achieved after eventually replacing the base field by some intermediate field in the cyclotomic \mathbb{Z}_p -extension.

If $k > 0$ is such that $\mu_{p^k} \subset \mathbb{K}$ but $\mu_{p^{k+1}} \not\subset \mathbb{K}$ then we set the numeration of the fields to be $\mathbb{K} = \mathbb{K}_1 = \dots = \mathbb{K}_k \subsetneq \mathbb{K}_{k+1}$. We recall from Definition 3 in [4], that $x \in A^-$ is called of λ -, of μ - or of finite type, according to whether Λx has finite rank, infinite rank and finite order, or is finite, respectively. The modules $L, M \subset A$ are the modules of elements of λ - resp of μ -types, and they both contain by definition the finite type elements. In the cyclotomic \mathbb{Z}_p -extension of CM fields we always have $L^- \cap M^- = 0$. Elements $x \in A$ that split as a sum of an element of λ - and one of μ -type are called decomposed and they build the module $D \subset A$, with $[A : D] < \infty$.

1.2. Thaine shift and the main coherent sequences. We define here the fields and modules which will be used for the proof. Let \mathbb{K} be a galois CM extension constructed as above. Let in particular $a \in M^-(\mathbb{K}) \setminus \mathfrak{MM}^-(\mathbb{K})$ a norm coherent sequence with $\text{ord}(a) = p^B = \exp(M^-(\mathbb{K}))$, $B > 2$ so $\Lambda a \sim \Lambda/p^B \Lambda$. There is some smallest integer ℓ which depends only on a , such that

$$(1) \quad p^j a \notin T^\ell p^j A^-(\mathbb{L}) + p^{j+1} A^-(\mathbb{K}) \quad \text{for all } 0 \leq j < B,$$

and a can be chosen such that ℓ is minimal under all possible choices. We can assume that the choice of \mathbb{K} is such that we have $Tx \in D^-(\mathbb{K})$ for all $x \in A^-(\mathbb{K})$ with $p^{B+1}x \in L^-(\mathbb{K})$, with $p^B = \exp(M^-(\mathbb{K}))$. We assume without loss of generality that $B > 2$, see also the remark at the end of the next section.

Let $m > k$ be some large integer, the size of which will be fixed in the next chapter, and let $\mathfrak{q} \in a_m^{1/2}$ be a prime which is totally split in \mathbb{K}_m/\mathbb{Q} and inert in $\mathbb{K}_\infty/\mathbb{K}_m$ and let $\mathbb{F} \subset \mathbb{Q}[\zeta_q]$ be the subfield of degree p in the q -th cyclotomic extension and $\mathbb{L} = \mathbb{K} \cdot \mathbb{F}$ be the inert Thaine shift induced by \mathfrak{q} . The galois group $F = \text{Gal}(\mathbb{F}/\mathbb{Q})$ is a cyclic group of order p , generated by $\nu \in F$, and we write $s := \nu - 1$. The algebraic norm

$$(2) \mathcal{N} := \sum_{i=0}^{p-1} \nu^i = pu(s) + s^{p-1} = p + sf(s), \quad f \in \mathbb{Z}_p[X], \quad u \in (\mathbb{Z}_p[s])^\times.$$

The arithmetic norm will be denoted by $\mathcal{N}_a = \mathbf{N}_{\mathbb{L}/\mathbb{K}} = \mathbf{N}_{\mathbb{L}_n/\mathbb{K}_n} = \mathbf{N}_{\mathbb{F}/\mathbb{Q}}, \forall n$. Then we may choose $b = (b_l)_{l \in \mathbb{N}} \in A^-(\mathbb{L})$ such that

- A. Let $\mathfrak{Q} \subset \mathbb{L}_m$ be the ramified prime above \mathfrak{q} . Then $b_m := [\mathfrak{Q}/\overline{\mathfrak{Q}}]$.
- B. For all $l > m$ we have $\mathcal{N}(b_l) = a_l$. In particular, $a = \mathcal{N}(b)$ and $pb_l = a_l; sb_l = 0$ for $l \leq m$.
- C. If $p^{B+1}b \in L^-(\mathbb{L})$ then $Tb \in D^-(\mathbb{L})$.

The last condition follows from Lemma 4 in [4]. Let $B'_n \subset A^-(\mathbb{L}_n)$ be the submodule spanned by the classes of primes that ramify in $\mathbb{L}_n/\mathbb{K}_n$. By choice of \mathbb{L} , these are the primes above q and consequently $B'_n = \iota_{m,n}(B'_m)$ for all $n > m$. Defining $p^b := \exp(B'_m)$ we have a fortiori $p^b B'_n = 0$ for all $n \geq m$. The notation introduced here will be kept throughout the paper.

1.3. Auxiliary facts. We present a variant of a fact that was proved in [4], providing a self contained proof.

Lemma 1. *There is a sequence $\gamma \in A^-(\mathbb{L})$ such that*

$$(3) \quad \text{Ker}(\mathcal{N} : A^-(\mathbb{L}) \rightarrow A^-(\mathbb{L})) = \Lambda\gamma + sA^-(\mathbb{L}).$$

Moreover, $p\text{-rk}(H^1(F, A^-(\mathbb{L}_n))) = [\mathbb{L}_m^- : \mathbb{Q}]$ and $d = \deg(\omega_m)$ is the smallest integer with $T^d\gamma \in sA^-(\mathbb{L})$. Finally, for any $x \in \text{Ker}(\mathcal{N} : A^-(\mathbb{L}') \rightarrow A^-(\mathbb{L}'))$ there is a $h = h(x) \in A^-(\mathbb{L}) \setminus sA^-(\mathbb{L})$, together a $c \geq 0$ and $w \in A^-(\mathbb{L})$ such that $x = T^c\gamma + sw$, while

$$(4) \quad T^{p^m}h = s\varpi \in sA^-(\mathbb{L}) \quad \text{and} \quad ph = s^{p-1}\rho, \quad \psi, \rho \in A^-(\mathbb{L}).$$

Proof. Let $q \in \mathbb{N}$ be the prime below \mathfrak{q} ; by definition, we have $v_p(q-1) = m$ and $\mathcal{O}(\mathbb{K}_n)/(q) \cong \prod_{g \in G_m} \mathbb{F}_{q^{p^n-m}}$, with $G_m = \text{Gal}(\mathbb{K}_m/\mathbb{Q})$ the galois group acting on the inert prime $\mathfrak{q}_n := \mathfrak{q}\mathcal{O}(\mathbb{L}_n)$ and $\mathbb{F}_{q^{p^n-m}} \cong \mathcal{O}(\mathbb{K}_n)/(\mathfrak{q}_n)$ being the corresponding subfield of the (unramified) \mathbb{Z}_p -extension of \mathbb{Q}_q .

The Hasse Norm Principle implies that $x \in \mathbb{K}_n^\times$ is a norm from \mathbb{L}_n iff it is a norm at all the primes above q ; the local norm defect is a subgroup of order p in $\mathbb{F}_q^\times[\zeta_{p^n}]$ and a generator thereof may be identified with ξ_n , with

$$(5) \quad \xi_n \equiv \begin{cases} \zeta_{p^n} \bmod \mathfrak{q}_n & \text{and} \\ 1 \bmod g\mathfrak{q}_n & \text{for all } g \in G_m, g \neq 1. \end{cases}$$

Let $r_n := \xi_n/\bar{\xi}_n$ and $R_n = \mathbb{F}_p[G_n]r_n + q\mathcal{O}(\mathbb{K}_n^\times)$. We claim that $H^1(F, A^-(\mathbb{L}_n)) \cong R_n$. To see this, note first that $pH^1(F, A^-(\mathbb{L}_n)) = 0$ so $H^1(F, A^-(\mathbb{L}_n))$ is an \mathbb{F}_p -module on which G_n acts. We next construct an isomorphism $\psi : R_n \rightarrow H^1(F, A^-(\mathbb{L}_n))$. The projections of interest will be denoted by $\pi : A^-(\mathbb{L}_n) \rightarrow H^1(F, A^-(\mathbb{L}_n))$ and $\pi' : \mathbb{K}_n^\times \rightarrow R_n$.

Let $\rho \in \mathbb{K}_n$ generate a prime $(\rho) \subset \mathbb{K}_n$ with $\rho - \xi_n \in q\mathcal{O}(\mathbb{K}_n)$ and which is totally split in \mathbb{L}_n/\mathbb{Q} , and let $\mathfrak{R} \subset \mathbb{L}_n$ be a prime above (ρ) . By definition, we have $\mathcal{N}(\mathfrak{R}^{1-j}) = (\rho/\bar{\rho})$ and \mathfrak{R}^{1-j} cannot be principal, since otherwise $\rho/\bar{\rho} \in \mathcal{N}(\mathbb{L}_n^\times)$, which contradicts the choice of ρ and of ξ_n . We obtain thus a map of $\mathbb{F}_p[G_m^+]$ -modules $\psi : R_n^{1-j} \rightarrow H^1(F, A^-(\mathbb{L}_n))$. The same argument shows that the kernel is trivial, since for $\psi(r/\bar{r}) = 1$, the above construction leads to $r = 1$. The map is also surjective: indeed, if $x \in \text{Ker}(\mathcal{N} : A^-(\mathbb{L}_n) \rightarrow A^-(\mathbb{L}_n))$ and $\mathfrak{X} \in x$ then $\mathcal{N}(\mathfrak{X}^{1-j}) = (u/\bar{u})$ for some $u \in \mathbb{L}_n^\times$. Assume that the image $v = u + q\mathcal{O}(\mathbb{K}_n)$ verifies $v = \bar{v}$; then $u/\bar{u} \in \mathcal{N}(\mathbb{L}_n)$, so let $\mathcal{N}(\mathfrak{X}^{1-j}) = (\mathcal{N}(y)), y \in \mathbb{L}_n^\times$. Then $\mathcal{N}(\mathfrak{X}^{1-j}/(y)) = (1)$ and there is an ideal $\mathfrak{Y} \subset \mathbb{L}_n$ with $\mathfrak{Y}^s = \mathfrak{X}^{1-j}/(y)$. It follows that $x \in (A^-(\mathbb{L}_n))^s$ and, denoting the image of $\bar{x} = x + (A^-(\mathbb{L}_n))^s \in H^1(F, A^-(\mathbb{L}_n))$,

we see that $\bar{x} = 1$ if there is an ideal $\mathfrak{X} \in x$ with $\mathcal{N}(\mathfrak{X}^{1-j}) \in \mu_{p^n} \mathcal{N}(\mathbb{L}_n)$. This implies that ψ is surjective, confirming the claim.

There is a norm coherent sequence $\gamma_n \in A^-(\mathbb{L}_n)$, $n \in \mathbb{N}$ such that $\bar{\gamma}_n \in H^1(F, A^-(\mathbb{L}_n))$ generates the $\mathbb{F}_p[G_m]$ -cyclic module. The claim follows by noticing that one may choose a sequence ξ_n , such that the images $\pi'(\xi^{1-j})_n$ are norm coherent. This completes the proof of the first claim, since

$$(p, \omega_m)H^1(F, A^-(\mathbb{L}_n)) = 0 \quad \text{for all } n, \text{ while } T^{d-1}\gamma_n = \nu_{m,1}\gamma_n \neq 0.$$

Finally, let $x \in \text{Ker}(\mathcal{N} : A^-(\mathbb{L}') \rightarrow A^-(\mathbb{L}'))$, let n' be large and and $\pi(x_{n'}) = g(T)\gamma_{n'} + sw_{n'}, w_{n'} \in A^-(\mathbb{L}_{n'})$. We claim that $x - g(T)\gamma \in sA^-$; indeed, $x - g(T)\gamma - sw \in \nu_{n',1}A^-(\mathbb{L})$ and for $n > n' > m$ we have $\nu_{n,1}H^1(F, A^-(\mathbb{L}_n)) = 0$, thus $\nu_{n',1}A^-(\mathbb{L}) \subset sA^-(\mathbb{L})$, which confirms the claim that $x = T^c\gamma + sw$. The identity (4) is a direct consequence. \square

We have the following strengthening of the previous result:

Lemma 2. *Notations being like above, $\text{Ker}(\mathcal{N} : M^-(\mathbb{L}) \rightarrow M^-(\mathbb{L})) \subset sM^-(\mathbb{L})$. Moreover,*

$$(6) \quad \text{Ker}(s : A^-(\mathbb{L}) \rightarrow A^-(\mathbb{L})) = \iota(A^-(\mathbb{K}))$$

Proof. We first prove that $H^0(F, A^-(\mathbb{L})) = 0$, which is equivalent to (6). Consider $x = (x_n)_{n \in \mathbb{N}} \in \text{Ker}(s : A^-(\mathbb{L}) \rightarrow A^-(\mathbb{L}))$ and let $N > m + n_0(\mathbb{L})$. If $\mathfrak{X} \in x_N$ then $(\mathfrak{X}^{s(1-j)}) = (\xi^{1-j})$, for some $\xi \in \mathbb{L}_N$ and $\mathcal{N}(\xi^{1-j}) \in \mu(\mathbb{K}_N)$. Since \mathfrak{q}_m is inert in $\mathbb{K}_N/\mathbb{K}_m$, we have $\mathcal{N}(\mathbb{L}_N) \cap \mu(\mathbb{K}_N) \subset \mu(\mathbb{K}_N)^p$. We may thus assume, after eventually modifying ξ by a root of unity, that $\mathcal{N}(\xi^{1-j}) = 1$. Hilbert's Theorem 90 implies that there is some $\gamma/\bar{\gamma} \in \mathbb{L}_N^{1-j}$ such that

$$\mathfrak{X}^{s(1-j)} = (\xi^{1-j}) = (\gamma^{1-j})^s \Rightarrow (\mathfrak{X}/(\gamma))^{(1-j)s} = (1).$$

Consequently, the class x_N contains a product of ramified ideals. Recall that $B'_N = \iota_{m,N}(B'_m)$ is spanned by the classes of the ramified primes and $p^b B'_N = 0$. In particular $x_N \in B'_N$ implies that $\mathbf{N}_{N,N-b}(x_N) = 0$. This happens for all N sufficiently large, so $\Lambda x \subset A^-(\mathbb{L})$ must be finite, which is absurd: A^- is free of finite torsion in cyclotomic \mathbb{Z}_p -extensions. This completes the proof of (6).

We let $\gamma_n \in A^-(\mathbb{L}_n)$ be defined in the previous lemma. We show that there is some $x \in L^-(\mathbb{L})$ such that $x \equiv \gamma \pmod{sA^-}$. In view of (6), $p\gamma_n = -s^{p-1}u^{-1}(s)\gamma_n$ and assuming without loss of generality that $\text{ord}(\gamma_n) > p$, we have $\Lambda[s]\gamma_n \cap A_n^-[p] \subset \text{Ker}(s : \Lambda[s]\gamma_n \rightarrow \Lambda[s]\gamma_n)$ and there must exist some non-trivial $k_n \in A^-(\mathbb{K}_n)[p] \cap s^{\mathbb{N}}\gamma_n$. Let $g(T) \in \mathbb{Z}_p[T]$ be the minimal monic, distinguished polynomial with $h := g(T)\gamma \in M^-(\mathbb{L})$.

Let $\mathbb{K}^{ab} := \mathbb{K} \cap \mathbb{Q}^{ab} \supseteq \mathbb{Q}[\zeta_{p^k}]$ and $N_a = \mathbf{N}_{\mathbb{K}/\mathbb{K}^{ab}}$, while $\mathbb{L}^{ab} = \mathbb{K}^{ab} \cdot \mathbb{F}$. Then N_a commutes with ν and we define $\chi := N_a(\gamma) \in A^-(\mathbb{L}^{ab})$. Since $\mathbb{L}^{(ab)}$ is abelian, the Theorem of Ferrero-Washington implies that χ is an element of λ -type. We may assume without loss of generality that the modules $A_n^-(\mathbb{K}^{ab})$ are stable beyond the base field, since this already holds for \mathbb{K} ,

so let $d = d_n(\chi) := p\text{-rk}(\Lambda\chi_n)$. We note that $H^1(F, A^-(\mathbb{L}^{(ab)}))$ is also a cyclic $\mathbb{F}_p[\text{Gal}(\mathbb{L}_m^{(ab),+}/\mathbb{Q})]$ -module which is annihilated by ω_m but not by $\omega_m/T = \nu_{m,1}$. This follows from the arguments used in the proof of Lemma 1 for showing $\nu_{m,1}H^1(F, A^-(\mathbb{L}_n)) \neq 0$, by using the fact that the prime $Q = \mathfrak{q} \cap \mathbb{L}_m^{(ab)}$ is totally split.

We claim that $d \geq p^{m-k} = \deg(\omega_m(T))$. Indeed, if $e := \deg(f_\chi) \leq \deg(\nu_{m,1}) < \deg(\omega_m(T))$ and $\pi(\chi) \in H^1(F, A^-(\mathbb{L}^{(ab)}))$ then $f_\chi(T)\pi(\chi) = T^e\pi(\chi) = 0$ and a fortiori $\nu_{m,1}\pi(\chi) = 0$, in contradiction with the choice of χ . On the other hand, we assumed that $h = g(T)\gamma \in M^-(\mathbb{L})$ and thus $N_a(h) = 0$, also a consequence of the Theorem of Ferrero-Washington. Thus

$$N_a(h) = N_a(g(T)\gamma) = g(T)N_a(\gamma) = g(T)\chi = 0.$$

By the above, we must have $\deg(g) \geq \deg(\omega_m)$. But then $h = g(T)\gamma \in sA^-(\mathbb{L}) \cap M^- = sM^-$, as a consequence of Lemma 1. This completes the proof of the first claim too. \square

Remark 1. Let K be a CM extension with $\mu^{(c)} > 0$. We show that it is possible to build a further CM extension \mathbb{L}/K with $\exp(M^-(\mathbb{L})) > p^2$. We have shown that we may assume without restriction of generality that $\mu_{p^2} \subset K$. Let $a \in M^-(K)$ and $\mathfrak{q} \in a_2$, with $a_2 \neq 0$, be a totally split prime which is inert in K_∞/K_2 . Let \mathbb{L}/K_2 be the inert Thaine shift of degree p^2 induced by \mathfrak{q} , let $b_2 = [\mathfrak{Q}^{(1-j)/2}]$ be the class of the ramified prime of \mathbb{L} above \mathfrak{q} and $b = (b_m)_{m \in \mathbb{N}}$ be a sequence through b_2 and such that $N_{\mathbb{L}/K}(b) = a$. Then $b \notin L^-(\mathbb{L})$ and there is some polynomial $f(T) \in \mathbb{Z}_p[T]$ such that $f(T)b \in M^-(\mathbb{L})$, while $\mathbf{N}_{\mathbb{L}/K}(f(T)b) = f(T)a$. Since \mathbb{L}/K is a Kummer extension, the capitulation kernel $\text{Ker}(\iota : A^-(K_n) \rightarrow A^-(\mathbb{L}))$ is \mathbb{Z}_p -cyclic. Consequently $\text{ord}(Tf(T)b) \geq p^2\text{ord}(a)$ and thus $\exp(M^-(\mathbb{L})) > p^2$.

2. ON THE VANISHING OF μ

The idea of the proof is simple: since $sb_m = 0$ we have $sb = \nu_{m,1}x$ for some $x \in A^-(\mathbb{L})$. Imagine that we had $b = \nu_{m,1}y + sz$: this would immediately lead to a contradiction to the choice of a . A careful work with the Tate cohomologies show that reality is quite more complex, but there is a contradiction of this very quality, which follows from the assumption $\mu^-(\mathbb{K}) > 0$. By reflection, it follows also that $\mu^+(\mathbb{K}) = 0$.

Recall that decomposition is granted in $TA^-(\mathbb{K})$, but in $A^-(\mathbb{L})$ it depends upon the exponent of $M^-(\mathbb{L})$. The following result is a partial indication for unconditional decomposition in \mathbb{L} .

Lemma 3. Let $b \in A^-(\mathbb{L}) \setminus \text{Ker}(\mathcal{N})$; then either $Tb \in D^-$ or $p\mathcal{N}(b) \in L^-(\mathbb{K})$.

Proof. Let $p^B = \exp(M^-(\mathbb{K}))$ and $b \in (M^-(\mathbb{L}) \cap \mathbf{B}) \setminus \mathfrak{M}(M^-(\mathbb{L}))$ have norm $a = \mathcal{N}(b)$. We shall show that $p^{B+1}b \in L^-(\mathbb{L})$, possibly unless $pa \in L^-(\mathbb{K})$. In the first case, the choice of \mathbb{K} implies that $Tb \in D^-(\mathbb{L})$, which will confirm the statement of this lemma.

Herewith, the claim of the lemma is that if $pa \neq 0$, then $\text{ord}(b) \leq p \text{ord}(a)$. We assume that $b \in M^-(\mathbb{L})$, which can always be achieved upon multiplication by a distinguished polynomial, and without modification of the L -order of the element ¹ – according to $\text{ord}_L(x) = \text{ord}(f_x(T)x)$.

We choose N large, so that $\text{ord}(b) = \text{ord}(b_N)$ and $N > k$ and consider the module $B_N := \mathbb{Z}_p[s]b_N \subset M_N^-(\mathbb{L})$; we write for simplicity $B := B_N$ only in this proof. Letting $A = \mathbb{Z}_p a_N = \mathbb{Z}_p \mathcal{N}b_N$, we obtain the couple (A, B) which is a $\mathbb{Z}_p[s]$ -module *transition*; the galois action relates the p -rk(B) to the growth factor $\text{ord}(b_N)/\text{ord}(a_N)$ in a way which we analyze below.

Since $s\mathcal{N} = 0$, there is a minimal monic, distinguished annihilator polynomial $f(s) \in \mathbb{Z}_p[s]$ of b_N and its degree is $\deg(f) < p$. Moreover, $\text{ord}(b_N) \leq \exp(M^-(\mathbb{L}))$ is uniformly bounded for all N , so $|B| \leq \exp(M^-(\mathbb{L}))^p$ is uniformly bounded. The subgroup $B'_N \subset \iota_{m,N}(A^-(\mathbb{L}_m))$. We claim that for N sufficiently large we always have $B \cap B'_N = 0$. Assume this is not the case and let $x = g(s)b_N = \sigma\iota(b_m) \in B'_N \cap \mathcal{R}$. Since $r_m = \sigma b_m$ is fixed by ω_m , we have $x_{N-b} = \mathbf{N}_{N,N-b}(x) = g(s)b_{N-b} = p^b r_m = 0$ for $N > 2(m+b)$, say. It follows that $g(s)b \in \nu_{N-b,1}A^-(\mathbb{L})$. However, $\mathbb{Z}_p[s]b$ is a finite module, since it has finite p -rank and we assumed $b \in M^-(\mathbb{L})$ so it has finite exponent too. Therefore, for sufficiently large N , we have $\nu_{N-b,1}A^-(\mathbb{L}_N) \cap \mathbb{Z}_p[s]b_N = 0$, which confirms the claim $B \cap B'_N = 0$.

It follows that $|H^0(F, B)| = 0$ and since B is finite, $|H^1(F, B)| = |H^0(F, B)| = 0$ too. In particular B/pB and $B[p]$ are both $\mathbb{F}_p[s]$ -cyclic modules. Let $d = p\text{-rk}(B)$ and $\bar{b} \in B/pB$ be the image of b_N , so $(s^i \bar{b})_{i=0, d-1}$ have independent images in B/pB by definition of the rank, and span B as a consequence of the Nakayama Lemma. Therefore $s^d \bar{b} \in pB$ and there is a monic distinguished annihilator polynomial $f(s) = s^d - p^e h(s)$ of b_N , with $e \geq 0$ and h a polynomial of $\deg(h) < \deg(f) \leq p$, which is not p -divisible.

If $d < p-1$, then $e > 0$ and

$$\begin{aligned} a_N &= \mathcal{N}(b_N) = pu(s)b_N + s^{p-1}b_N = p(u(s) + s^{p-1-d}p^{e-1}h(s))b_N \\ &= pv(s)b_N, \quad v(s) \in (\mathbb{Z}_p[s])^\times, \end{aligned}$$

so $a_N = v^{-1}(s)a_N = pb_N$, thus $\text{ord}(b_N) = p \cdot \text{ord}(a_N)$, and we are done.

If $d = p-1$, then $s^{p-1}b_N = p \cdot (p^{e-1}h(s))b_N$ and thus

$$a_N = (pu(s) + s^{p-1})b_N = p(u(s) + p^{e-1}h(s))b_N$$

and if the expression in the brackets is a unit, we may conclude like before. Otherwise, $e = 1$ and $h(s) = -1 + sh_1(s)$. We obtain, after clearing singularities, $a = s^{c'}p^{d'}h_2(s)b_N$ with $c' > 0, d' \geq 0$ and $h_2 \in \mathbb{Z}_p[s]$ with $h_2(0) \neq 0$ and not p -divisible. We obviously have $pa_N = \mathcal{N}(a_N) = \mathcal{N}(O(s)) = 0$, so we are in the exceptional case $pa_N = 0$, which completes the investigation of the case $d = p-1$.

Finally, suppose that $d = p$. There is an exact sequence of $\mathbb{F}_p[s]$ -modules $1 \rightarrow B[p] \rightarrow B \rightarrow B/pB \rightarrow 1$ in which B/pB is cyclic generated by b_N .

¹For $x \in A^-$ we define the L -order by $\text{ord}_L(x) = \min\{p^e \geq 1 : p^e x \in L^-\}$

It follows that $B[p]$ is also $\mathbb{F}_p[s]$ -cyclic. Since $d = p$, we have $p\text{-rk}(B) = p$ and $s^{p-1}b_N = a_N - pb_N u(s) \notin pB$; in particular $a_N \notin pB$. If $pa_N = 0$ or $p\text{ord}(a_N)b_N = 0$ there is nothing to show, so we assume that $\text{ord}(a_N) = q$ with $v_p(q) > 1$ and $\text{ord}(b_N) = p^e q, e > 1$. We note that $\text{ord}(s^{p-1}b_N) = p^{e-1}q$, since $s^{p-1}u^{-1}(s)b_N = -pb_N - a_N$ has annihilator $p^{e-1}q$. There is thus some $0 \leq j < p-1$ such that $\text{ord}(s^j b_N) = \text{ord}(b_N) > \text{ord}(s^{j+1}b_N) = \text{ord}(b_N)/p$. Let

$$\begin{aligned}\mathcal{F}_0 &:= \{qp^{e-1}s^i b_N : i = 0, 1, \dots, j\}, \\ \mathcal{F}_1 &:= \{qp^{e-2}s^{j+i}b_N : i = 0, 1, \dots, p-j-1\} \subset B[p],\end{aligned}$$

and $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1$. Then $\mathcal{F}_i \subset B[p]$ are \mathbb{F}_p -bases of some cyclic $\mathbb{F}_p[s]$ submodules $F_0, F_1 \subset B[p]$. We have $\dim_{\mathbb{F}_p}(F_0) + \dim_{\mathbb{F}_p}(F_1) = p = \dim_{\mathbb{F}_p}(B)$. Since for each $x \in B[p]$ there is some $y \in B/pB$ with $x = ry$ and $r \in p^{\mathbb{N}}$ we conclude that $F_0 \cup F_1 \supset B$; therefore $B = F_0 \oplus F_1$ as an \mathbb{F}_p -vector space. Note that

$$0 \neq (q/p)a_N = qb_N + (q/p)s^{p-1}u^{-1}(s)b_N \in B[p][s];$$

upon multiplication with p^{e-1} we obtain $0 = qp^{e-2}a_N = qp^{e-1}b_N + qp^{e-2}(s^{p-1} + O(s^p))b_N$. Since B is $\mathbb{F}_p[s]$ -cyclic and $s^{p-1}qp^{e-2}b_N \in F_1[s]$, we have $s^p qp^{e-2}b_N = qp^{e-1}b_N v(s), v \in (\mathbb{F}_p[s])^\times$. Assembling these relations we obtain

$$0 = qp^{e-2}s^{p-1}b_N + f_0, \quad f_0 \in F_0.$$

This implies $qp^{e-2}s^{p-1}b_N \in F_0 \cap F_1$, which contradicts the rank condition established previously, and completes the proof. \square

We let now a, b be as described. Since we assumed that $\text{ord}(a) = p^B > p^2$ and this order is maximal in $M^-(\mathbb{K})$, it follows that $p\mathcal{N}(b) = pa \notin L^-(\mathbb{K})$. The Lemma 3 implies that $Tb \in D^-(\mathbb{L})$. Assume first that we even have $b \in M^-(\mathbb{L})$, so $b_\lambda = 0$ and $b_\mu = Tb$. Then $sb_m = 0$ implies, by Lemma 1, we have $Tsb = \omega_m d$ with $d \in A^- \cap \text{Ker}(\mathcal{N} : M^- \rightarrow M^-)$. Thus $d = sd'$ by Lemma 2 and $s(Tb - \omega_m d') = 0$. Since $\text{Ker}(s) = A^-(\mathbb{K})$, it follows that $Tb = \omega_m d' + y, y \in A^-(\mathbb{K})$. The norm yields $Ta = \omega_m \mathcal{N}(d') + py \in (T^P, p)A^-(\mathbb{K})$, $P = \deg(\omega_m)$. For sufficiently large m , this contradicts the choice of a .

The simpler case $b \in \mathbb{M}^-(\mathbb{L})$ readily illustrates the approach of our proof: assuming some $a \in M^-(\mathbb{K})$ chosen appropriately, we find a *deformation* $b \in A^-(\mathbb{L})$ in an inert Thaine shift, which has norm $\mathcal{N}(b) = a$ and such that $sb_j = 0$ for all $j \leq m$ and m fixed, but arbitrarily large. The choices of a and b reveal eventually a contradiction which shows that $M^-(\mathbb{K}) = 0$. By Kummer duality, it follows that $M^+(\mathbb{K}) = 0$ too, so $M(\mathbb{K}) = 0$, which will complete the proof.

The case when b is undecomposed is more complex, but will be led to the same type of contradiction, using the Lemma 3. We shall make repeatedly use of the fact that $A^-(\mathbb{L})$ has no finite torsion submodule, in the proof below. This implies that $L^-(\mathbb{L}) \cap M^-(\mathbb{L}) = 0$ and if $c(T)x \in M^-$ for $c(T) \in \Lambda \setminus p\Lambda$, then $x \in M^-$.

Proof. In this case we still have $sb_m = 0$. By Iwasawa's Theorem 6 (also Lemma 2 in [4]) there is a $x \in A^-(\mathbb{L})$ with $sb = \nu_{m,1}x$ and $\nu_{m,1}\mathcal{N}(x) = 0$, so Sands's result Lemma 15 in [4] implies that $x \in \text{Ker}(\mathcal{N})$. An application of Lemma 1 implies the existence of $c \geq 0$ and $d \in A^-(\mathbb{L})$, such that $x = T^k h + sd$ and thus $sb = \nu_{m,1}T^c h + \nu_{m,1}sd$ and $T^{c+\deg(\nu_{m,1})}h \in sA^-(\mathbb{L})$. We may assume that $\nu_{m,1}T^c h = g_1(T)\psi$, with ψ defined in Lemma 1. We obtain

$$s(b - g_1(T)\psi - \nu_{m,1}d) = 0 \quad \Rightarrow \quad b = g_1(T)\psi + \nu_{m,1}d + y, \quad y \in A^-(\mathbb{K}).$$

After applying T to the above identity and using the fact that Ty, Tb are decomposed, we obtain:

$$\delta := g_1(T)T\psi + \omega_m d = (b_\lambda - y_\lambda) + (b_\mu - y_\mu) \in D^-(\mathbb{L}).$$

We have in fact $p^{B+1}\delta = p^{B+1}T(b - y) \in L$. We claim that $p^{B+1}d, p^{B+1}\psi \in L^-(\mathbb{L})$ too. Indeed, let $F(T)$ be a distinguished polynomial of minimal degree such that $\psi' := F(T)\psi$, $d' := F(T)d \in M^-(\mathbb{L})$ and $g(T) = Tg_1(T)$. Then $\delta' := g(T)\psi' + \omega_m d'$ is such that $p^{B+1}\delta' \in L^-(\mathbb{L}) \cap M^-(\mathbb{L}) = 0$, i.e. $\delta' \in M^-(\mathbb{L})[p^{B+1}]$. Assume that $\psi' \notin M^-(\mathbb{L})[p^{B+1}]$, so $d' \notin M^-(\mathbb{L})[p^{B+1}]$ either. Let $f = \deg(F)$, $P = \deg(\omega_m)$, $e = \deg(g(T))$; from $TF(T)a = \mathcal{N}(\delta') - pTF(T)y$ and the definition (1) of ℓ , we see that $\deg(g) \leq \ell$. However, if $p^{B+1+j} = \text{ord}(\psi')$ then $p^{B+j}(\delta') \in M^-(\mathbb{L})[p]$, while $p^{B+j}g(T)\psi' \notin T^{\ell+1}M^-(\mathbb{L})[p]$ by choice of ℓ and due to $p^{B+j}\omega_m d \in T^P M^-(\mathbb{L})[p]$. Therefore $p^{B+j}\delta' \neq 0$, while we know that $p^{B+1}\delta' = 0$: it follows that $j = 0$, which confirms our claim, and thus $p^{B+1}\psi, p^{B+1}d \in L^-(\mathbb{L})$. If we could argue that $L^-(\mathbb{L}_n)$ is stable from the first level, we could deduce from this that $Th, T\psi \in D^-(\mathbb{L})$. However, \mathbb{L} depends on the choice of m and this the rank stabilization is not fixed by \mathbb{K} . We must take a different approach and show first that the claim follows if we *assume* that

$$(7) \quad Td, Th \in D^-(\mathbb{L}).$$

Then $Th = h_\lambda + h_\mu \in D^-(\mathbb{L})$. Since $h \in \text{Ker}(\mathcal{N})$, we see that $\mathcal{N}(h_\lambda) = -\mathcal{N}(h_\mu)$ and the separation of λ and μ -parts yields $\mathcal{N}(h_\mu) = 0$, so the Lemma 2 implies $h_\mu = sw, w \in M^-(\mathbb{L})$.

In this case $Tsb = s(b_\lambda + b_\mu) = \nu_{m,1}(g_1(T)h_\lambda + g_1(T)h_\mu + sd_\lambda + sd_\mu)$ and thus $s(b_\mu - \nu_{m,1}(d_\mu + w)) = 0$. The vanishing of $\text{Ker}(s)$ yields $b_\mu = \nu_{m,1}(w + d) + y, y \in M^-(\mathbb{K})$. Taking norms again, we obtain the same contradiction as in the case $b \in M^-(\mathbb{L})$.

The claim of the Theorem follows herewith, if we show that (7) must hold. We shall relate the sequences d, ψ to $a, A^-(\mathbb{K})$. Since we have shown that $p^{B+1}\psi, p^{B+1}d \in L^-$, it follows that $p^{B+1}\omega_n h \in L^-(\mathbb{L})$ and thus $p^{B+1}h \in L^-$ too. By Lemma 3, the condition (7) is thus true unless $p\mathcal{N}(\psi) \in L^-(\mathbb{L})$ or $p\mathcal{N}(d) \in L^-(\mathbb{L})$; we have to investigate therefore these two cases. In either case we have

$$p(b_\lambda + b_\mu) = p(\delta_\lambda + \delta_\mu) + p(y_\lambda + y_\mu),$$

and since $\mathcal{N}(b_\lambda) = Ta_\lambda = 0$, we have

$$(8) \quad pTa = p\mathcal{N}(\delta_\mu) + p^2y_\mu = p(g(T)\mathcal{N}(\psi) + \omega_m\mathcal{N}(d)_\mu) + p^2y_\mu;$$

The above identity being one of μ -parts, it follows that if $p\mathcal{N}(\psi) \in L^-(\mathbb{K})$ then $p\mathcal{N}(\delta_\mu) = p\mathcal{N}(\omega_md)_\mu$ and $pTa = p(\omega_n\mathcal{N}(d))_\mu + p^2y_\mu$. Consequently, $pTa \in pT^PA^- \bmod (p^2A^-(\mathbb{K}))$ which contradicts the choice of a and ℓ . This eliminates the case $p\mathcal{N}(\psi) \in L^-(\mathbb{K})$.

It remains that $p\mathcal{N}(d) \in L^-(\mathbb{K})$ and $p\mathcal{N}(\psi) \notin L^-(\mathbb{K})$. We have shown after (7) that Th is decomposed and $h_\mu = sw; w \in M^-(\mathbb{L})$. We do not know whether d is decomposed, but certainly ω_md is. And for its μ -part we have $(\omega_nd)_\mu \in T^PA^-(\mathbb{L}) + pA^-(\mathbb{L})$ while $p(\omega_n\mathcal{N}d)_\mu = 0$, since $p\mathcal{N}(d) \in L^-(\mathbb{K})$. Using this we find

$$\begin{aligned} Tsb &= T\nu_{m,1}(g(T)h + sd), \quad \text{hence} \\ sb_\mu &= s(\nu_{m,1}(g(T)w + (\nu_{m,1}d)_\mu)) \quad \text{so} \\ p\mathcal{N}(b_\mu) &= p\nu_{m,1}\mathcal{N}(g(T)w) + (p\mathcal{N}(\nu_{m,1}d))_\mu + p^2y_\mu \\ &= p\nu_{m,1}\mathcal{N}(g(T)w) + p^2y_\mu = pTa. \end{aligned}$$

Consequently $pTa = p\nu_{m,1}\mathcal{N}(g(T)w) + p^2y_\mu$. It follows in this case that $pa \equiv pg(T)T^{P-1} \bmod p^2A^-(\mathbb{K})$, which likewise contradicts the definition of ℓ . This completes the proof of $\mu = 0$. \square

Acknowledgements: The main proof idea was first investigated in the wish to present the result in the memorial volume [1] for Alf van der Poorten. However not more than the trivial case was correctly proved; Sören Kleine undertook within part of his PhD Thesis the task of brushing up the proof. He succeeded to do so, with the exception of the details related to decomposition, which we treated here. I owe to Sören Kleine for numerous useful discussion sustained during the development of this paper. I dedicate the paper to the memory of Alf van der Poorten.

REFERENCES

- [1] J. Borwein, I. Shparlinski, and W. Zudilin, editors. *Number Theory and Related Fields: In Memory of Alf van der Poorten*. Springer, 2013.
- [2] B. Ferrero and L. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Annals of Mathematics (2)*, (109):377–395, 1979.
- [3] K. Iwasawa. On the μ -invariants of cyclotomic fields; in honor of Y. Akizuki. pages 1–11, Kinokuniya, Tokyo, 1973.
- [4] P. Mihăilescu. On CM \mathbb{Z}_p -extensions and the Leopoldt conjecture for CM fields. Math. Arxiv, May 2014. <http://front.math.ucdavis.edu/XXXX>.

(P. Mihăilescu) MATHEMATISCHES INSTITUT DER UNIVERSITÄT GÖTTINGEN
E-mail address, P. Mihăilescu: preda@uni-math.gwdg.de